kaspersky

Kaspersky Security Center 17 Linux

© 2026 АО "Лаборатория Касперского"

Содержание

Справка Kaspersky Security Center Linux

Что нового

Исправленные ошибки

О Kaspersky Security Center Linux

- Комплект поставки
- Аппаратные и программные требования
  - Требования Сервера администрирования
  - Требования Web Console
  - Требования Агента администрирования
- Совместимые приложения и решения "Лаборатории Касперского"
- О совместимости компонентов Kaspersky Security Center Linux
- Сравнение версий Kaspersky Security Center: на базе Windows и на базе Linux
- О Kaspersky Security Center Cloud Console

Архитектура и основные понятия

- Архитектура приложения
- Схема развертывания Сервера администрирования Kaspersky Security Center Linux и Kaspersky Security Center Web Console
- Порты, используемые Kaspersky Security Center Linux
- Порты, используемые приложением Kaspersky Security Center Web Console
- Основные понятия
  - Сервер администрирования
  - Иерархия Серверов администрирования
  - Виртуальный Сервер администрирования
  - Веб-сервер.
  - Веб-сервер Kaspersky Security Center Linux
  - Агент администрирования
  - Группы администрирования
  - Управляемое устройство
  - Нераспределенное устройство
  - Рабочее место администратора
  - Веб-плагин управления
  - Политики
  - Профили политик
  - Задачи
  - Область действия задачи
  - Взаимосвязь политики и локальных параметров приложения
  - Точка распространения
  - Шлюз соединения
  - Виртуальные Серверы администрирования

Схемы трафика данных и использования портов

- Сервер администрирования и управляемые устройства в локальной сети (LAN)
- Главный Сервер администрирования в локальной сети (LAN) и два подчиненных Сервера администрирования
- Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете: использование обратного прокси-сервера

Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете; использование шлюза соединения
Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете
Взаимодействие компонентов Kaspersky Security Center Linux и приложений безопасности: дополнительные сведения
Условные обозначения в схемах взаимодействия
Сервер администрирования и СУБД
Сервер администрирования и клиентское устройство: Управление приложением безопасности
Обновление программного обеспечения на клиентском устройстве с помощью точки распространения
Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования
Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне
Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство
Сервер администрирования и два устройства в демилитаризованной зоне: шлюз соединений и клиентское устройство
Сервер администрирования и Kaspersky Security Center Web Console
Начало работы
Руководство по усилению защиты
Контрольный список по усилению защиты
Развертывание Сервера администрирования
Безопасность соединения
Учетные записи и авторизация
Управление защитой Сервера администрирования
Управление защитой Агента администрирования
Управление защитой клиентских устройств
Настройка защиты управляемых приложений
Обслуживание Сервера администрирования
Передача событий в сторонние системы
Рекомендации по безопасности сторонних информационных систем
Рекомендации по использованию приложений безопасности "Лаборатории Касперского"
Сценарий: аутентификация MySQL Server
Сценарий: двухсторонняя TLS-аутентификация PostgreSQL для базы данных Сервера администрирования и базы данных IAM
Подготовка к развертыванию
Выбор конфигурации Kaspersky Security Center Linux
Типовая конфигурация: один офис
Типовая конфигурация: несколько крупных офисов с собственными администраторами
Типовая конфигурация: множество небольших удаленных офисов
Выбор структуры защиты организации
Типовые способы развертывания системы защиты
Выбор СУБД
Предоставление доступа к Серверу администрирования из интернета
Доступ из интернета: Сервер администрирования в локальной сети
Доступ из интернета: Сервер администрирования в демилитаризованной зоне
Установка
Настройка сервера MariaDB x64 для работы с Kaspersky Security Center Linux
Настройка сервера СУБД на основе PostgreSQL для работы с Kaspersky Security Center Linux
Настройка сервера MySQL x64 для работы с Kaspersky Security Center Linux
Подготовка кластера высокой доступности СУБД для работы с Kaspersky Security Center Linux

Установка Kaspersky Security Center Linux
Установка Kaspersky Security Center Linux в тихом режиме
Установка Kaspersky Security Center Linux на Astra Linux в режиме замкнутой программной среды
Установка Kaspersky Security Center Web Console
Параметры установки Kaspersky Security Center Web Console
Установка Kaspersky Security Center Web Console на Astra Linux в режиме замкнутой программной среды
Установка Kaspersky Security Center Linux с помощью скрипта
Развертывание отказоустойчивого кластера Kaspersky Security Center Linux
Отказоустойчивый кластер Kaspersky Security Center Linux. Схемы развертывания
Отказоустойчивый кластер Kaspersky Security Center Linux
Сценарий: развертывание отказоустойчивого кластера Kaspersky Security Center Linux
Отказоустойчивый кластер Kaspersky Security Center Linux. Аппаратные и программные требования
Подготовка файлового сервера для отказоустойчивого кластера Kaspersky Security Center Linux
Подготовка узлов для отказоустойчивого кластера Kaspersky Security Center Linux
Установка Kaspersky Security Center Linux на узлы отказоустойчивого кластера Kaspersky Security Center Linux
Запуск и остановка узлов кластера вручную
Переустановка узла отказоустойчивого кластера
Установка Kaspersky Security Center Web Console, подключенной к Серверу администрирования, установленного на узлах отказоустойчивого кластера Kaspersky Security Center Linux
Геораспределенный отказоустойчивый кластер Kaspersky Security Center Linux
Геораспределенный кластер под управлением Ubuntu с СУБД PostgreSQL
Подготовка файловой системы узлов кластера
Настройка реплицированной файловой системы кластера
Установка и настройка Corosync и Pacemaker на узлах кластера
Установка и настройка СУБД PostgreSQL
Установка Kaspersky Security Center Linux на узлы геораспределенного отказоустойчивого кластера
Геораспределенный кластер под управлением SberLinux с СУБД Platform V Pangolin
Подготовка файловой системы узлов кластера
Настройка реплицированной файловой системы кластера
Установка и настройка Corosync и Pacemaker на узлах кластера
Установка и настройка СУБД Platform V Pangolin
Установка Kaspersky Security Center Linux на узлы геораспределенного отказоустойчивого кластера
Установка Kaspersky Security Center Web Console на узлы геораспределенного отказоустойчивого кластера
Учетные записи для работы с СУБД
Создание баз и учетных записей СУБД MySQL и MariaDB
Создание баз и учетных записей СУБД на основе PostgreSQL
Перенос данных из общего табличного пространства в табличное пространство file-per-table в СУБД MySQL или MariaDB
Сертификаты для работы с Kaspersky Security Center Linux
О сертификатах Kaspersky Security Center
Требования к пользовательским сертификатам, используемым в Kaspersky Security Center Linux
Перевыпуск внутренних сертификатов для Kaspersky Security Center Web Console
Замена сертификата для Kaspersky Security Center Web Console
Преобразование сертификата из формата PFX в формат PEM
Сценарий: задание пользовательского сертификата Сервера администрирования
Замена сертификата Сервера администрирования с помощью утилиты klsetsrvcert
Подключение Агентов администрирования к Серверу администрирования с помощью утилиты klmover

Перевыпуск сертификата Веб-сервера
Замена IAM-сертификата по умолчанию на пользовательский сертификат
Добавление адреса Сервера администрирования в конфигурацию сервера IAM
Задание папки общего доступа
Вход в приложение Kaspersky Security Center Web Console и выход из него
Интерфейс Kaspersky Security Center Web Console
Изменение языка интерфейса Kaspersky Security Center Web Console
Изменение домашней страницы Kaspersky Security Center Web Console
Добавление и удаление закладок
Удаление Kaspersky Security Center Web Console
Мастер первоначальной настройки
Шаг 1. Указание параметров подключения к интернету
Шаг 2. Загрузка требуемых обновлений
Шаг 3. Выбор активов для защиты
Шаг 4. Выбор шифрования
Шаг 5. Настройка установки плагинов для управляемых приложений
Шаг 6. Загрузка дистрибутивов и создание инсталляционных пакетов
Шаг 7. Настройка Kaspersky Security Network
Шаг 8. Выбор способа активации приложения
Шаг 9. Указание параметров управления обновлениями приложений сторонних производителей
Шаг 10. Создание базовой конфигурации защиты сети
Шаг 11. Настройка параметров отправки уведомлений по электронной почте
Шаг 12. Завершение работы мастера первоначальной настройки
Мастер развертывания защиты
Шаг 1. Запуск мастера развертывания защиты
Шаг 2. Выбор инсталляционного пакета
Шаг 3. Выбор способа распространения файла ключа или кода активации
Шаг 4. Выбор версии Агента администрирования
Шаг 5. Выбор устройств
Шаг 6. Задание параметров задачи удаленной установки
Шаг 7. Управление перезагрузкой
Шаг 8. Удаление несовместимых приложений перед установкой
Шаг 9. Перемещение устройств в папку Управляемые устройства
Шаг 10. Выбор учетных записей для доступа к устройствам
Шаг 11. Запуск установки
Обновление предыдущей версии Kaspersky Security Center Linux
Обновление Kaspersky Security Center Linux версии 16 или выше
Обновление Kaspersky Security Center Linux версии 16 или выше с помощью установочного файла
Обновление Kaspersky Security Center Linux версии 16 или выше с помощью резервной копии
Обновление Kaspersky Security Center Linux версии 16 или выше на узлах отказоустойчивого кластера Kaspersky Security Center Linux
Обновление Kaspersky Security Center Linux версии 15.4 или ниже
Обновление Kaspersky Security Center Linux версии 15.4 или ниже с помощью установочного файла
Обновление Kaspersky Security Center Linux версии 15.4 или ниже с помощью резервной копии
Обновление Kaspersky Security Center Linux с версии 15.4 или ниже на узлах отказоустойчивого кластера Kaspersky Security Center Linux

Обновление Kaspersky Security Center Web Console
Обновление Kaspersky Security Center Web Console на Astra Linux в режиме замкнутой программной среды
Перенос данных в приложение Kaspersky Security Center Linux
Сценарий миграции на Kaspersky Security Center Linux с использованием скрипта быстрой установки
Общее руководство по миграции на новый сервер Kaspersky Security Center Linux
Перенос данных в Kaspersky Security Center с помощью мастера переноса данных
Экспорт групповых объектов из Kaspersky Security Center Windows
Импорт файла экспорта в Kaspersky Security Center Linux
Переключение управляемых устройств под управление Kaspersky Security Center Linux
Настройка Сервера администрирования
Настройка адреса подключения Сервера администрирования
Настройка параметров подключения Kaspersky Security Center Web Console к Серверу администрирования
Настройка списка разрешенных IP-адресов для подключения к Kaspersky Security Center Linux
Настройка параметров доступа Сервера администрирования к интернету
Иерархия Серверов администрирования
Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования
Просмотр списка подчиненных Серверов администрирования
Управление виртуальными Серверами администрирования
Создание виртуального Сервера администрирования
Включение и выключение виртуального Сервера администрирования
Назначение администратора виртуального Сервера администрирования
Смена Сервера администрирования для клиентских устройств
Удаление виртуального Сервера администрирования
Настройка журнала событий подключения к Серверу администрирования
Настройка количества событий в хранилище событий
Перенос Сервера администрирования на другое устройство
Смена имени Сервера администрирования
Сохранение подключений с помощью добавления новой записи DNS
Сохранение подключений с помощью переключения на основе IP-адреса
Восстановление прерванных подключений после изменения имени Сервера
Изменение учетных данных СУБД
Резервное копирование и восстановление данных Сервера администрирования
Создание задачи резервного копирования данных Сервера администрирования
Использование утилиты klbackup для резервного копирования и восстановления данных
Использование утилиты klbackup для переключения управляемых устройств под управление другого Сервера администрирования
Резервное копирование и восстановление данных Сервера администрирования при использовании MySQL или MariaDB
Обслуживание Сервера администрирования
Удаление иерархии Серверов администрирования
Доступ к общедоступным DNS-серверам
Настройка интерфейса
Защищенное подключение к Серверу администрирования
Шифрование подключения TLS
Сетевые параметры для взаимодействия с внешними сервисами
Глобальный список подсетей
Проверка целостности модулей с помощью утилит klscmodchk и integrity_checker

Обнаружение устройств в сети
Сценарий: обнаружение сетевых устройств
Опрос сети Windows
Опрос IP-диапазонов
Добавление и изменение IP-диапазона
Опрос Zeroconf
Опрос контроллеров домена
Аутентификация и подключение к контроллеру домена
Настройка доменной аутентификации для Сервера администрирования с помощью флагов
Настройка контроллеров домена Samba
Инвентаризация оборудования
Добавление информации о новых устройствах
Настройка критериев определения корпоративных устройств
Использование динамического режима VDI на клиентских устройствах
Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования
Перемещение в группу администрирования устройств, являющихся частью VDI
Управление клиентскими устройствами
Параметры управляемого устройства
Проверка соединения клиентского устройства с Сервером администрирования вручную Утилита klnagchk
Правила перемещения устройств
Создание правил перемещения устройств
Копирование правил перемещения устройств
Условия для правила перемещения устройств
Добавление устройств в состав группы администрирования вручную
Перемещение устройств или кластеров в состав группы администрирования вручную
О кластерах и массивах серверов
Свойства кластеров или массивов серверов
Настройка точек распространения и шлюзов соединений
О точках распространения
Типовая конфигурация точек распространения: один офис
Типовая конфигурация точек распространения: множество небольших удаленных офисов
Расчет количества и конфигурации точек распространения
Автоматическое назначение точек распространения
Назначение точек распространения вручную
Добавление шлюза соединения в демилитаризованной зоне в качестве точки распространения
Изменение списка точек распространения для группы администрирования
Включение push-сервера
Увеличение ограничения дескрипторов файлов для службы klnagent
О статусах устройства
Настройка переключения статусов устройств
Выборки устройств
Просмотр списка устройств из выборки устройств
Создание выборки устройств
Настройка выборки устройств
Экспорт списка устройств из выборки устройств
Удаление устройств из групп администрирования в выборке

- Теги устройств
  - Создание тегов устройств
  - Изменение тегов устройств
  - Удаление тегов устройств
  - Просмотр устройств, которым назначен тег
  - Просмотр тегов, назначенных устройству
  - Назначение тегов устройству вручную
  - Удаление назначенного тега с устройства
  - Просмотр правил автоматического назначения тегов устройствам
  - Изменение правил автоматического назначения тегов устройствам
  - Создание правил автоматического назначения тегов устройствам
  - Выполнение правил автоматического назначения тегов устройствам
  - Удаление правил автоматического назначения тегов с устройств
  - Управление тегами устройств с помощью утилиты klscflag
- Шифрование и защита данных
  - Просмотр списка зашифрованных жестких дисков
  - Просмотр списка событий шифрования
  - Формирование и просмотр отчетов о шифровании
  - Предоставление доступа к зашифрованному жесткому диску в автономном режиме
  - Передача ключей шифрования между Серверами администрирования
- Смена Сервера администрирования для клиентских устройств
- Избегание конфликтов между Серверами администрирования
- Перемещение устройств, подключенных к Серверу администрирования через шлюзы соединения, на другой Сервер администрирования
- Просмотр и настройка действий, когда устройство неактивно
- Отправка сообщения пользователям устройств
- Удаленное включение, выключение и перезагрузка клиентских устройств
- Удаленный доступ к управляемым устройствам
  - Удаленный доступ с Linux-устройства с Kaspersky Security Center Web Console к управляемому Linux-устройству
  - Удаленный доступ с Linux-устройства с Kaspersky Security Center Web Console к управляемому Windows-устройству
  - Удаленный доступ с Windows-устройства с Kaspersky Security Center Web Console к управляемому Linux-устройству
  - Удаленный доступ с Windows-устройства с Kaspersky Security Center Web Console к управляемому Windows-устройству
- Управление мобильными устройствами
  - Использование Firebase Cloud Messaging
  - Интеграция с инфраструктурой открытых ключей

Управление группами администрирования

- Создание групп администрирования
- Автоматическая установка приложений на устройства группы администрирования
- Перемещение групп администрирования
- Удаление групп администрирования

Развертывание приложений "Лаборатории Касперского"

- Сценарий: развертывание приложений "Лаборатории Касперского"
- Добавление плагина управления для приложений "Лаборатории Касперского"

Инсталляционные пакеты
- Загрузка и создание инсталляционных пакетов для приложений "Лаборатории Касперского"
- Создание инсталляционных пакетов из файла
- Создание автономного инсталляционного пакета
- Параметры инсталляционного пакета Агента администрирования
- Запуск автономных пакетов, сформированных Kaspersky Security Center Linux
- Установка приложений с помощью автономных пакетов
- Целесообразность обновления баз в инсталляционном пакете приложения безопасности
- Изменение ограничения на размер пользовательского инсталляционного пакета
- Распространение инсталляционных пакетов на подчиненные Серверы администрирования
- Просмотр списка автономных инсталляционных пакетов

Установка Агента администрирования для Linux
- Подготовка устройства с операционной системой Linux к установке Агента администрирования
- Подготовка устройства под управлением SUSE Linux Enterprise Server 15 к установке Агента администрирования
- Подготовка устройства под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования
- Подготовка к установке Агента администрирования на устройство с операционной системой Linux с glibc 2.5 (устаревшая операционная система)
- Подготовка к установке Агента администрирования на устройство с операционной системой OpenSSH версии 6.4 (устаревшая операционная система)
- Удаленная установка Агента администрирования на устройство с операционной системой Linux
- Установка Агента администрирования для Linux в тихом режиме (с файлом ответов)
- Установка Агента администрирования для Linux в интерактивном режиме
- Поддержка отката файловой системы для устройств с Агентом администрирования

Установка Агента администрирования для Windows
- Установка Агента администрирования для Windows в интерактивном режиме
- Установка Агента администрирования для Windows в тихом режиме
- Развертывание захватом и копированием образа устройства
- Режим клонирования диска Агента администрирования
- Параметры установки Агента администрирования

Установка приложений с помощью задачи удаленной установки
- О задачах удаленной установки приложений Kaspersky Security Center Linux
- Удаленная установка приложений
- Удаленная установка приложений на устройства с операционной системой macOS
- Установка приложений на подчиненные Серверы администрирования
- Удаленная установка приложений на устройства с установленным Агентом администрирования
- Управление перезагрузкой устройств в задаче удаленной установки
- Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center Linux
- Установка приложений в тихом режиме

Подготовка устройства с операционной системой macOS к удаленной установке Агента администрирования

Виртуальная инфраструктура
- Рекомендации по снижению нагрузки на виртуальные машины
- Поддержка динамических виртуальных машин
- Поддержка копирования виртуальных машин

Указание параметров удаленной установки на устройствах под управлением Unix

Мониторинг развертывания

Запуск и остановка приложений "Лаборатории Касперского"

- Замещение приложений безопасности сторонних производителей
- Удаленная деинсталляция приложений или обновлений программного обеспечения
- Подготовка устройства под управлением Windows к удаленной установке
- Создание задачи Удаленное выполнение скриптов
  - Создание инсталляционного пакета на основе манифест-файла
  - Подготовка архива для задачи Удаленное выполнение скриптов
  - Удаленная установка приложений на устройства с помощью задачи Удаленное выполнение скриптов
  - Настройка уведомлений и мониторинга для задачи Удаленное выполнение скриптов

Лицензирование

- Лицензирование Kaspersky Security Center Linux
  - О Лицензионном соглашении
  - О лицензии
  - О Лицензионном сертификате
  - О лицензионном ключе
  - Просмотр Политики конфиденциальности
  - Варианты лицензирования Kaspersky Security Center
  - О файле ключа
  - О предоставлении данных
  - О подписке
  - Активация Kaspersky Security Center Linux
- Лицензирование управляемых приложений "Лаборатории Касперского"
  - Лицензирование управляемых приложений
  - Добавление лицензионного ключа в хранилище Сервера администрирования
  - Распространение лицензионного ключа на клиентские устройства.
  - Автоматическое распространение лицензионного ключа.
  - Просмотр информации об используемых лицензионных ключах
  - События превышения лицензионного ограничения
  - Удаление лицензионного ключа из хранилища
  - Отзыв согласия с Лицензионным соглашением
  - Продление срока действия лицензии приложений "Лаборатории Касперского"
  - Использование Kaspersky Marketplace для выбора бизнес-решений

Настройка приложений "Лаборатории Касперского"

- Сценарий: настройка защиты сети
- Подходы к управлению безопасностью, ориентированные на устройства и на пользователей
- Настройка и распространение политик: подход, ориентированный на устройства
- Настройка и распространение политик: подход, ориентированный на пользователя
- Политики и профили политик
  - О политиках и профилях политик
  - Блокировка (замок) и заблокированные параметры
  - Наследование политик и профилей политик
    - Иерархия политик
    - Профили политик в иерархии политик
    - Как параметры реализованы на управляемом устройстве
  - Управление политиками
    - Просмотр списка политик
    - Создание политики
    - Общие параметры политик

Изменение политики
Включение и выключение параметра наследования политики
Копирование политики
Перемещение политики
Экспорт политики
Импорт политики
Принудительная синхронизация
Просмотр диаграммы состояния применения политики
Автоматическая активация политики по событию "Вирусная атака"
Удаление политики
Управление профилями политик
Просмотр профилей политики
Изменение приоритета профиля политики
Создание профиля политики
Копирование профиля политики
Создание правила активации профиля политики
Удаление профиля политики
Экспорт и импорт профиля политики
Параметры политики Агента администрирования
Использование Агента администрирования для Windows, Linux и macOS: сравнение
Сравнение параметров Агента администрирования по операционным системам
Включение и выключение режима низкого потребления ресурсов для Агента администрирования
Настройка параметров защиты управляемых приложений
Ручная настройка групповой задачи обновления Kaspersky Endpoint Security
Ручная настройка групповой задачи проверки устройства Kaspersky Endpoint Security
Kaspersky Security Network (KSN)
О KSN
Настройка доступа к KSN
Включение и выключение использования KSN
Просмотр принятого Положения о KSN
Принятие обновленного Положения о KSN
Проверка, работает ли точка распространения как прокси-сервер KSN
Просмотр статистики работы прокси-сервера KSN
Управление задачами
О задачах
Область задачи
Создание задачи
Запуск задачи вручную
Запуск задачи для выбранных устройств
Просмотр списка задач
Общие параметры задач
Экспорт задачи
Импорт задачи

Запуск мастера изменения паролей задач
Шаг 1. Выбор учетных данных
Шаг 2. Выбор выполняемого действия
Шаг 3. Просмотр результатов
Просмотр результатов выполнения задач, хранящихся на Сервере администрирования
Теги приложений
Теги приложений
Создание тегов приложений
Изменение тегов приложений
Назначение тегов приложениям
Снятие назначенных тегов с приложений
Удаление тегов приложений
Использование утилиты klscflag для открытия порта 13291
Регистрация приложения Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center Web Console
Управление пользователями и ролями пользователей
Об учетных записях пользователей
О ролях пользователей
Настройка прав доступа к функциям приложения. Управление доступом на основе ролей
Права доступа к функциям приложения
Предопределенные роли пользователей
Назначение прав доступа к набору объектов
Назначение прав пользователям или группам безопасности
Добавление учетной записи внутреннего пользователя
Создание группы безопасности
Изменение учетной записи внутреннего пользователя
Изменение группы безопасности
Назначение роли пользователю или группе безопасности
Добавление учетных записей пользователей во внутреннюю группу безопасности
Назначение пользователя владельцем устройства
Назначение пользователя владельцем устройства при установке Агента администрирования
Назначение пользователя владельцем устройства Linux после установки Агента администрирования
Отмена назначения пользователя владельцем устройства
Включение защиты учетной записи от несанкционированного изменения
Настройка двухфакторной аутентификации
О двухфакторной аутентификации учетной записи
Настройка секретного ключа двухфакторной аутентификации при входе в Kaspersky Security Center Web Console
Разрешение для настройки двухфакторной аутентификации пользователям
Сброс и удаление секретного ключа двухфакторной аутентификации
Исключение учетных записей из двухфакторной аутентификации
Изменение имени издателя кода безопасности
Изменение количества попыток ввода пароля
Удаление пользователей или групп безопасности
Изменение пароля учетной записи пользователя
Создание роли пользователя
Изменение роли пользователя
Изменение области для роли пользователя
Удаление роли пользователя

- Связь профилей политики с ролями
- Распространение пользовательских ролей на подчиненные Серверы администрирования
- Смена пароля учетной записи
- Отзыв прав локального администратора
- Настройка доменной аутентификации Kerberos

Обновление баз и приложений "Лаборатории Касперского"
- Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"
- Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"
- Создание задачи Загрузка обновлений в хранилище Сервера администрирования
- Проверка полученных обновлений
- Создание задачи загрузки обновлений в хранилища точек распространения
- Добавление источников обновлений для задачи Загрузка обновлений в хранилище Сервера администрирования
- Одобрение и отклонение обновлений программного обеспечения
- Автоматическая установка обновлений для Kaspersky Endpoint Security для Windows
- Об использовании файлов различий для обновления баз и модулей приложений "Лаборатории Касперского"
- Включение функции загрузки файлов различий
- Загрузка обновлений точками распространения
- Обновление баз и модулей приложений "Лаборатории Касперского" на автономных устройствах

Мониторинг, отчеты и аудит
- Сценарий: мониторинг и отчеты
- О типах мониторинга и отчетах
- Срабатывание правил в режиме Интеллектуального обучения
  - Просмотр и подтверждение обнаружений, выполненных с помощью правил Адаптивного контроля аномалий
  - Добавление исключений в правила Адаптивного контроля аномалий
- Панель мониторинга и виджеты
  - Использование панели мониторинга
  - Добавление виджета на информационную панель
  - Удаление виджета с информационной панели
  - Перемещение виджета на информационной панели
  - Изменение размера или внешнего вида виджета
  - Изменение параметров виджета
  - О режиме Просмотра только панели мониторинга
  - Настройка режима Просмотра только панели мониторинга
- Отчеты администрирования и защиты
  - Использование отчетов
  - Создание шаблона отчета
  - Просмотр и изменение свойств шаблона отчета
  - Экспорт отчета в файл
  - Генерация и просмотр отчета
  - Создание задачи рассылки отчета
  - Удаление шаблонов отчетов
- Центр усиления безопасности
  - Установлено приложение безопасности
  - Политика применена
  - Обновление антивирусных баз настроено
  - Резервное копирование настроено
  - Обслуживание Сервера администрирования настроено

- Шифрование TLS включено
- Все устройства управляемые

События и выборки событий
- О событиях в Kaspersky Security Center Linux
- События компонентов Kaspersky Security Center Linux
  - Структура данных описания типа события
  - События Сервера администрирования
    - Критические события Сервера администрирования
    - События отказа функционирования Сервера администрирования
    - События предупреждения Сервера администрирования
    - Информационные события Сервера администрирования
  - События Агента администрирования
    - События отказа функционирования Агента администрирования
    - События предупреждения Агента администрирования
    - Информационные события Агента администрирования
- Использование выборок событий
- Создание выборки событий
- Изменение выборки событий
- Просмотр списка выборки событий
- Экспорт выборки событий
- Импорт выборки событий
- Просмотр информации о событии
- Экспорт событий в файл
- Просмотр истории объекта из события
- Удаление событий
- Удаление выборок событий
- Настройка срока хранения события
- Блокировка частых событий
  - О блокировке частых событий
  - Управление блокировкой частых событий
  - Отмена блокировки частых событий
- Обработка и хранение событий на Сервере администрирования

Уведомления и статусы устройств
- Об уведомлениях
- Просмотр уведомлений, требующих внимания
- Просмотр системных уведомлений
- Просмотр объявлений
- Выключение объявлений "Лаборатории Касперского"
- Настройка переключения статусов устройств
- Настройка параметров доставки уведомлений
- Проверка распространения уведомлений
- О статусах устройства
- Параметры и переменные среды для описания события

Просмотр информации об обнаруженных угрозах

Интеграции для реагирования на алерты
Настройка интеграции с Active Directory для выполнения действий по реагированию
Настройка интеграции с Kaspersky Automated Security Awareness Platform
Настройка интеграции с Kaspersky Threat Intelligence Portal Sandbox
Группировка алертов по атрибутам
Cloud Discovery
Включение функции Cloud Discovery с помощью виджета
Добавление виджета Cloud Discovery в панель мониторинга
Просмотр информации об использовании облачных сервисов
Уровень риска облачных сервисов
Блокировка доступа к нежелательным облачным сервисам
Экспорт событий в SIEM-системы
Настройка экспорта событий в SIEM-системы
Предварительные условия
Об экспорте событий
О настройке экспорта событий в SIEM-системе
Об экспорте событий в форматах CEF и LEEF
Конвертация событий в формат CEF или LEEF
Выбор событий для экспорта в SIEM-системы в формате Syslog
Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog
Выбор общих событий для экспорта в формате Syslog
Об экспорте событий в формате Syslog
Настройка Kaspersky Security Center Linux для экспорта событий в SIEM-систему
Мониторинг изменений политики и профилей политик
Экспорт событий напрямую из базы данных
Выполнение SQL-запроса с помощью утилиты klsql2
Пример SQL-запроса, созданного с помощью утилиты klsql2
Просмотр имени базы данных Kaspersky Security Center Linux
Просмотр результатов экспорта
Работа с ревизиями объектов
Просмотр и сохранение ревизии политики
Сравнение ревизий политики
Откат изменений объекта к предыдущей ревизии
Активные угрозы
Дезинфекция необработанного файла
Скачивание необработанного файла
Удаление файлов из раздела Активные угрозы
Удаление объектов
Загрузка и удаление файлов из разделов Карантин и Файлы резервных копий
Загрузка файлов из разделов Карантин и Файлы резервного хранилища
Об удалении объектов из разделов Карантин, Файлы резервного хранилища или Активные угрозы
Управление приложением с помощью SNMP
Настройка службы snmpd в операционной системе
Включение и выключение уведомления по SNMP
Включение и выключение SNMP в Kaspersky Security Center Linux
Значения идентификаторов объектов для SNMP

Использование Kaspersky Security Center Linux по лицензии Kaspersky Security для бизнеса Профессиональный
Интеграции для реагирования на алерты
Настройка интеграции с Active Directory для выполнения действий по реагированию
Настройка интеграции с Kaspersky Automated Security Awareness Platform
Настройка интеграции с Kaspersky Threat Intelligence Portal Sandbox
Группировка алертов по атрибутам
Интеграция Kaspersky Security Center Web Console с другими решениями "Лаборатории Касперского"
Установка фонового соединения
Настройка соединения с прокси-сервером
Удаленная диагностика клиентских устройств
Открытие окна удаленной диагностики
Включение и выключение трассировки для приложений
Загрузка файла трассировки приложения
Удаление файлов трассировки
Загрузка параметров приложений
Загрузка системной информации с клиентского устройства
Загрузка журналов событий
Запуск, остановка и перезапуск приложения
Запуск удаленной диагностики Агента администрирования Kaspersky Security Center Linux и скачивание результатов
Запуск приложения на клиентском устройстве
Запуск удаленной диагностики на клиентском устройстве с операционной системой Linux
Управление сторонними приложениями и исполняемыми файлами на клиентских устройствах
Использование компонента Контроль приложений для управления исполняемыми файлами
Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах
Создание пополняемой вручную категории приложений
Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств
Создание категории приложений, в которую входят исполняемые файлы из выбранных папок
Просмотр списка категорий приложений
Добавление исполняемых файлов, связанных с событием, в категорию приложения
Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows
Получение и просмотр списка приложений, установленных на клиентских устройствах
О приложениях сторонних производителей
Установка обновлений приложений сторонних производителей
Сценарий: обновление приложений сторонних производителей
Варианты установки обновлений стороннего программного обеспечения
Параметры задачи поиска уязвимостей и требуемых обновлений
Создание задачи Поиск уязвимостей и требуемых обновлений
Просмотр информации о доступных обновлениях приложений сторонних производителей.
Экспорт списка доступных обновлений в файл
Одобрение и отклонение обновлений приложений сторонних производителей.
Создание задачи Установка требуемых обновлений и закрытие уязвимостей
Добавление правил для установки обновлений
Параметры задачи Установка требуемых обновлений и закрытие уязвимостей, указанные после создания задачи
Автоматическое обновление приложений сторонних производителей
Закрытие уязвимостей в приложениях сторонних производителей
Об обнаружении и закрытии уязвимостей в приложениях
Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей

Закрытие уязвимостей в приложениях сторонних производителей
Создание задачи Закрытие уязвимостей
Пользовательские исправления для уязвимостей в приложениях сторонних производителей
Просмотр информации об уязвимостях в приложениях, обнаруженных на всех управляемых устройствах
Просмотр информации об уязвимостях в приложениях, обнаруженных на выбранных управляемых устройствах
Просмотр статистики уязвимостей на управляемых устройствах.
Экспорт списка уязвимостей в приложениях в текстовый файл
Игнорирование уязвимостей в приложениях
Создание инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"
Просмотр и изменение параметров инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"
Параметры инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"
Закрытие уязвимостей в изолированной сети
Сценарий: закрытие уязвимостей в приложениях сторонних производителей в изолированной сети
О закрытии уязвимостей в приложениях сторонних производителей в изолированной сети
Настройка Сервера администрирования с доступом в интернет для закрытия уязвимостей в изолированной сети
Настройка изолированных Серверов администрирования для закрытия уязвимостей в изолированной сети
Передача исправлений и установка обновлений в изолированной сети
Выключение передачи патчей и установка обновлений в изолированной сети
Справочное руководство API
Лучшие практики для поставщиков услуг
Планирование развертывания Kaspersky Security Center Linux
Предоставление доступа к Серверу администрирования из интернета
Типовая конфигурация Kaspersky Security Center Linux
О точках распространения
Иерархия Серверов администрирования
Виртуальные Серверы администрирования
Развертывание и первоначальная настройка
Рекомендации по установке Сервера администрирования
Создание учетных записей для служб Сервера администрирования на отказоустойчивом кластере
Выбор СУБД
Указание адреса Сервера администрирования
Поддержка неактивных подключений
Развертывание Агента администрирования и приложений безопасности
Настройка защиты в сети организации-клиента
Ручная настройка политики Kaspersky Endpoint Security
Настройка политики в разделе Продвинутая защита
Настройка политики в разделе Базовая защита
Настройка политики в разделе Дополнительные параметры
Настройка политики в разделе Настройка событий
Ручная настройка групповой задачи обновления Kaspersky Endpoint Security
Ручная настройка групповой задачи проверки устройства Kaspersky Endpoint Security
Настройка расписания задачи Поиск уязвимостей и требуемых обновлений.
Ручная настройка групповой задачи установки обновлений и закрытия уязвимостей
Построение структуры групп администрирования и назначение точек распространения
Типовая конфигурация MSP-клиента: один офис
Типовая конфигурация MSP-клиента: множество небольших изолированных офисов

Иерархия политик, использование профилей политик
Иерархия политик
Профили политик
Задачи
Правила перемещения устройств
Категоризация программного обеспечения
Резервное копирование и восстановление параметров Сервера администрирования
Вышло из строя устройство с Сервером администрирования
Повреждены параметры Сервера администрирования или база данных
О профилях соединения для автономных пользователей
О переключении Агента администрирования на другой Сервер администрирования
Создание профиля соединения для автономных пользователей
Удаленный доступ к управляемым устройствам
Использование параметра "Не разрывать соединение с Сервером администрирования" для обеспечения постоянной связи между управляемым устройством и Сервером администрирования
О проверке времени соединения устройства с Сервером администрирования
О принудительной синхронизации
Руководство по масштабированию
Об этом руководстве
Ограничения Kaspersky Security Center Linux
Расчеты для Серверов администрирования
Расчет аппаратных ресурсов для Сервера администрирования
Аппаратные требования для СУБД и Сервера администрирования
Расчет места в базе данных
Расчет места на диске
Расчет количества и конфигурации Серверов администрирования
Рекомендации по подключению динамических виртуальных машин к Kaspersky Security Center
Расчеты для точек распространения и шлюзов соединений
Требования для точки распространения
Расчет количества и конфигурации точек распространения
Расчет количества шлюзов соединений
Хранение информации о событиях для задач и политик
Лучшие практики для Сервера администрирования, управляющего большим количеством устройств
Особенности и оптимальные параметры некоторых задач
Частота обнаружения устройств
Задачи резервного копирования данных Сервера администрирования и обслуживания базы данных
Групповые задачи обновления Kaspersky Endpoint Security
Задача Инвентаризации
Информация о нагрузке на сеть между Сервером администрирования и защищаемыми устройствами
Потребление трафика при выполнении различных сценариев
Средний расход трафика за сутки
Известные проблемы и ограничения
Обращение в Службу технической поддержки
Способы получения технической поддержки
Техническая поддержка через Kaspersky CompanyAccount
Получение файлов дампа Сервера администрирования
Источники информации о приложении

Глоссарий
- Cloud discovery
- FileTransferBridge
- HTTPS
- Identity and Access Manager (IAM)
- iOS MDM-устройство
- JavaScript
- Kaspersky Security Center Linux System Health Validator (SHV)
- Lightweight Nagent (LWNGT)
- Network Location Awareness (NLA)
- Provisioning-профиль
- SSL
- Агент администрирования
- Агент аутентификации
- Агент обновлений
- Административные права
- Администратор Kaspersky Security Center Linux
- Администратор клиента
- Администратор поставщика услуг
- Активный ключ
- Антивирусная безопасность сети
- Антивирусные базы
- Веб-сервер Kaspersky Security Center Linux
- Виртуальный Сервер администрирования
- Вирусная атака
- Владелец устройства
- Внутренние пользователи
- Восстановление
- Восстановление данных Сервера администрирования
- Группа администрирования
- Групповая задача
- Демилитаризованная зона (DMZ)
- Домашний Сервер администрирования
- Дополнительный ключ
- Доступное обновление
- Задача
- Задача для набора устройств
- Инсталляционный пакет
- Клиент Сервера администрирования (Клиентское устройство)
- Консоль администрирования
- Конфигурационный профиль
- Локальная задача
- Локальная установка
- Магазин приложений
- Настройки задачи
- Непосредственное управление приложением
- Несовместимое приложение

Обновление
Общий сертификат
Оператор Kaspersky Security Center
Параметры приложения
Политика
Поставщик услуг антивирусной защиты
Профиль
Рабочее место администратора
Резервное копирование данных Сервера администрирования
Ролевая группа
Ручная установка
Сервер iOS MDM
Сервер администрирования
Серверы обновлений "Лаборатории Касперского"
Сертификат Сервера администрирования
Состояние защиты
Состояние защиты сети
Срок действия лицензии
Удаленная установка
Управляемые устройства
Уровень важности патча
Уровень важности события
Уязвимость
Файл ключа
Хранилище резервных копий
Хранилище событий
Централизованное управление приложением
Широковещательный домен
Шлюз соединения
Информация о стороннем коде
Уведомления о товарных знаках

Справка Kaspersky Security Center Linux

Новые функции

- Что нового

Аппаратные и программные требования

- Требования Сервера администрирования
- Требования Web Console
- Требования Агента администрирования

Начало работы

- Установка
- Мастер первоначальной настройки
- Мастер развертывания защиты

Лицензирование и активация

- Активация Kaspersky Security Center Linux
- Лицензирование управляемых приложений

Развертывание и настройка

- Обнаружение устройств в сети
- Расчеты для точек распространения и/или шлюзов соединений
- Замещение приложений безопасности сторонних производителей
- Приложения "Лаборатории Касперского". Централизованное развертывание

- Настройка защиты сети
- Приложения "Лаборатории Касперского". Обновление баз и модулей приложений
- Настройка адреса подключения Сервера администрирования
- Перенос данных в приложение Kaspersky Security Center Linux
- Об обновлении предыдущей версии Kaspersky Security Center Linux

Monitoring

- Мониторинг и отчеты
- Cloud Discovery

Управление клиентскими устройствами

- Удаленный доступ к управляемым устройствам

Системное администрирование

- Обнаружение и закрытие уязвимостей в приложениях сторонних производителей

Дополнительные возможности

- Экспорт событий в SIEM-системы
- Просмотр статистики работы прокси-сервера KSN
- Руководство по масштабированию (только онлайн-справка)

Что нового

Kaspersky Security Center 17 Linux

В приложении Kaspersky Security Center 17 Linux реализовано несколько новых функций и улучшений:

- Сертификаты Web Console, IAM и Сервера администрирования теперь можно добавлять вручную и заменять автоматически без переустановки Web Console.
- При просмотре содержимого ревизии, а также при сравнении ревизий политик теперь доступны данные профилей политик.
- Теперь после запуска задачи для устройства или набора устройств можно перейти к ее свойствам и просмотреть результаты выполнения.
- В Центр усиления безопасности добавлен новый индикатор уровня защиты, позволяющий отслеживать устройства, управление которыми могло быть потеряно.
- В события, публикуемые Сервером администрирования для управляемых устройств, добавлена следующая информация о клиентских устройствах: DNS-имя (FQDN), NetBIOS-имя, IP-адрес и DisplayName.
- Расширены возможности аудита:
  - При переключении Агента администрирования на другой Сервер администрирования в Kaspersky Event Log теперь регистрируется событие. В событии указывается адрес нового Сервера администрирования и адрес шлюза при его наличии.
  - При импорте и копировании политик, а также при откате политики к выбранной ревизии теперь отправляются расширенные события.
- Улучшен пользовательский опыт:
  - Раздел **Теги** переименован в **Теги устройств**.
  - Раздел **Теги устройств** и его подразделы перенесены из раздела **Управление активами** в раздел **Хранилища**.
  - Добавлена возможность выгружать в файл все события из списка событий по устройству и из выборок событий.
- Скрипт быстрой установки Kaspersky Security Center Linux теперь поддерживает дополнительные варианты развертывания:
  - MySQL 8.4.10 с Ubuntu Server 26.04 LTS.
  - MariaDB 10.11.18 с CentOS Stream 10.
  - MariaDB 10.11.18 с РЕД ОС 8.
  - MariaDB 10.11.13 с Astra Linux 1.8.5.

- Сервер администрирования теперь поддерживает новые версии СУБД:
  - MariaDB 11.4.
  - MariaDB 11.8.
  - MariaDB 12.3.
  - Platform V Pangolin 7.2.0.
  - Platform V Pangolin 7.2.0 (кластер Built-in High Availability).
- Сервер администрирования и Web Console теперь поддерживают работу со следующими новыми версиями операционных систем:
  - Альт Сервер 11.
  - МосОС 15.6.
- Агент администрирования теперь поддерживает работу со следующими новыми версиями операционных систем:
  - Microsoft Windows 11 26H2 Home/Pro/Pro for Workstations/Enterprise/Education.
  - Microsoft Windows 10 IoT Enterprise версия 1507.
  - Debian GNU/Linux версии 12.10, 12.11, 12.14 (Bookworm) ARM.
  - Astra Linux Special Edition РУСБ.10015-16 (исполнение 2) (очередное обновление 8.1) E2K.
  - Astra Linux Special Edition РУСБ.10265-01 (очередное обновление 8.1) E2K.
  - Эльбрус 9.3.6 E2K.
  - Альт Рабочая станция 11.2 ARM.
  - Альт Сервер 11.1 ARM.
  - Альт СП Рабочая станция 10 E2K.
  - Альт СП Сервер 10 E2K.
  - Альт 8 СП Рабочая станция E2K.
  - Альт 8 СП Сервер E2K.
  - МСВСфера 9.5 Сервер.
  - МСВСфера 9.5 АРМ.
  - Amazon Linux 2023.
  - МосОС 15.6.

Kaspersky Security Center 16.3 Linux

В приложении Kaspersky Security Center 16.3 Linux реализовано несколько новых функций и улучшений:

- При изменении политики для каждого измененного параметра создается отдельное событие аудита. Эти события экспортируются в SIEM.
- В **функциональность экспорта событий в SIEM-системы** добавлена поддержка Kaspersky SIEM.
- Kaspersky Security Center Linux теперь поддерживает работу с решением Kaspersky Vulnerability Management.
- В соответствии с Руководством по усилению защиты разработана оптимизированная конфигурация Kaspersky Endpoint Security для Linux для установки на устройства с Сервером администрирования, Web Console и СУБД, а также для развертывания отказоустойчивого кластера Kaspersky Security Center Linux.
- При установке Kaspersky Security Center Linux теперь вы можете указать пользовательскую схему баз данных.
- В разделе **Мониторинг → Панель мониторинга** индикатор уровня защиты помогает оценить безопасность вашего Сервера администрирования и точек распространения. Если индикатор желтый или красный, необходимо выполнить действия для решения проблем, чтобы статус индикатора изменился на зеленый.
- Доступен упрощенный способ развертывания Kaspersky Security Center Linux. Теперь вы можете использовать установочный скрипт.
- Доступен специальный дистрибутив Агент администрирования для устаревших версий Linux с glibc версии 2.5 для поддержки следующих устаревших операционных систем:
  - CentOS 5.2.
  - CentOS 5.4.
  - CentOS 6.4.
  - CentOS 6.6.
  - Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.4) 64-разрядная.
- Агент администрирования теперь поддерживает работу со следующими новыми версиями операционных систем:
  - Microsoft Windows 11 IoT Enterprise 25H2 64-разрядная.
  - SberOS 3.6.1.
  - Ubuntu Server 26.04 LTS.

- Следующие СУБД больше не поддерживаются:
  - MySQL 5.7.
  - MariaDB 10.1.30.
- Улучшен пользовательский опыт:
  - Расширены возможности фильтрации таблиц **Задачи** и **Политики**. Теперь вы можете добавить несколько условий, используя логический оператор `OR`, а также использовать новый оператор, который позволяет выбрать несколько значений для одного свойства и отобразить записи, соответствующие хотя бы одному из указанных критериев.
  - В главном меню:
    - Доступен новый раздел **Управление программным обеспечением**. В раздел **Управление программным обеспечением** перенесены разделы: **Инсталляционные пакеты**, **Приложения "Лаборатории Касперского"**, **Сторонние приложения**, **Каталог приложений "Лаборатории Касперского"** и **Управление патчами**.
    - Разделы **Нераспределенные устройства** и **Оборудование** перенесены в раздел **Управление активами**.
    - Разделы **Задачи** и **Хранилища** перенесены на первый уровень меню.
    - Раздел **Резервные копии веб-плагина** больше не используется и удален из Web Console.

Kaspersky Security Center 16.2 Linux



Обзор новых возможностей версии 16.2. Видео

В приложении Kaspersky Security Center 16.2 Linux реализовано несколько новых функций и улучшений:

- Теперь в Kaspersky Security Center Web Console можно настроить шлюз соединения в демилитаризованной зоне (DMZ).

  Используйте параметр **Использовать шлюз соединения в демилитаризованной зоне по адресу** для настройки шлюза соединения.

- Улучшен алгоритм сохранения идентификатора устройства Агента администрирования (параметр `Device ID`) на устройствах Linux. Если серийный номер BIOS устройства, серийный номер материнской платы, идентификаторы диска хранения или MAC-адрес совпадают с уже известными, Сервер администрирования правильно определяет устройство как ранее обнаруженное после обновления операционной системы или изменения MAC-адреса.

- Добавлена поддержка геораспределенного отказоустойчивого кластера Kaspersky Security Center Linux с узлами, расположенными в разных центрах обработки данных. В конфигурации геораспределенного кластера все компоненты являются отказоустойчивыми.

- Теперь вы можете экспортировать события в SIEM-систему в форматах CEF или LEEF.

- Добавлена поддержка кластера PostgreSQL высокой доступности с Patroni для автоматического переключения в случае сбоя и HAProxy для балансировки нагрузки.

- Вы можете сравнить ревизии политики. Параметр доступен для политик Сервера администрирования, Агента администрирования, Kaspersky Endpoint Security для Windows (начиная с версии веб-плагина 14.0) и Kaspersky Endpoint Security для Mac (начиная с версии веб-плагина 12.2.1 Patch A). Список приложений "Лаборатории Касперского", поддерживающих эту функцию, будет расширен в следующих версиях.

- Теперь поддерживается SNMP. Вы можете предоставлять информацию, статистику и события Сервера администрирования приложениям сторонних производителей с помощью SNMP.

- Опрос сети Windows теперь поддерживается для точек распространения с операционной системой Windows.

- Доступен единый инсталляционный пакет Агента администрирования для Linux. Этот инсталляционный пакет включает версии для разных менеджеров пакетов и архитектур процессоров. Во время установки среда определяется автоматически и устанавливается соответствующий пакет Агента администрирования.

- В события добавлена информация об инициаторе команд, выполняемых на мобильных устройствах.

- Компонент NSQ удален из дистрибутива Kaspersky Security Center Web Console. Служба KSCWebConsoleMessageQueue.service больше не используется и будет удалена после обновления Kaspersky Security Center Web Console.

- Если у Сервера Администрирования нет доступа к хранилищу дистрибутивов приложений для удаленной установки, то перед созданием инсталляционных пакетов из файла для установки приложений на устройства Windows вам потребуется загрузить дополнительные модули с сайта "Лаборатории Касперского": Files for remote installation via Kaspersky Security Center (архивы ri_utils_win32.zip и ri_utils_arm64.zip).

- Агент администрирования теперь поддерживает 64-разрядную архитектуру Windows Arm. Совместимость с управляемыми приложениями можно проверить в соответствующей документации.

- Kaspersky Security Center Linux поддерживает работу с Kaspersky Sandbox.

- Улучшен пользовательский опыт:

  - Теперь вы можете удалить сразу все события из выборки событий и из списка событий устройства.

    Параметры **Выбрать все** и **Выбрать все на текущей странице** доступны в выборке событий и в списке событий устройства.

- Теперь вы можете вручную указать приоритет правила перемещения.

  Кнопка **Изменить приоритет** становится доступной при выборе правила перемещения и позволяет указать новый приоритет.

- Kaspersky Security Center Linux поддерживает работу с Platform V SberLinux OS Server (SLO) 9.6.
- Kaspersky Security Center Linux теперь поддерживает работу со следующими СУБД:
  - MySQL Standard Edition 8.4.
  - MySQL Enterprise Edition 8.4.
  - PostgreSQL 18.
  - Postgres Pro 18 (все редакции).
  - Postgres Pro 18 Enterprise (кластер Built-in High Availability).
- Агент администрирования теперь поддерживает работу со следующими новыми версиями операционных систем:
  - Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM.
  - Platform V SberLinux OS Server (SLO) 9.6.

Kaspersky Security Center 16.1 Linux

В приложении Kaspersky Security Center 16.1 Linux реализовано несколько новых функций и улучшений:

- Двухфакторная аутентификация теперь включена по умолчанию. Глобальный параметр, выключающий двухфакторную аутентификацию, больше недоступен. Чтобы пользователи могли входить в Kaspersky Security Center Web Console и работать со скриптами автоматизации OpenAPI, перед обновлением необходимо включить двухфакторную аутентификацию для всех пользователей.
- Теперь профиль политики можно сохранить в файл KLPROF без экспорта политики, а затем использовать этот файл KLPROF для импорта сохраненного профиля в политику.
- Агент администрирования теперь может работать на устройствах под управлением ОС Альт в режиме закрытой программной среды.
- Добавлена поддержка доменной аутентификации на основе Kerberos для доменных пользователей без пароля с использованием протокола SCRIL, что позволяет реализовать технологию единого входа (SSO) на основе сертификатов.
- Улучшен пользовательский опыт:
  - Фильтрация клиентских устройств по версии операционной системы и менеджеру пакетов теперь учитывает версии операционных систем Linux.
  - Усовершенствовано отображение таблиц в Kaspersky Security Center Web Console: число элементов на страницу по умолчанию увеличено до 50, а настроенное число элементов теперь сохраняется от сеанса к сеансу.

- Комментарии к категориям приложений позволяют добавлять описания правил включения и исключения приложений в категории.
- По умолчанию в списке доступных инсталляционных пакетов теперь отображаются только инсталляционные пакеты приложений "Лаборатории Касперского" на языке интерфейса Kaspersky Security Center Web Console и на английском языке.

- Kaspersky Security Center Linux поддерживает работу с Kaspersky Endpoint Security для Linux 12.4.
- Kaspersky Security Center Linux поддерживает работу со следующими новыми версиями операционных систем:
  - Debian GNU/Linux 13 (Trixie).
  - CentOS Stream 10.
  - Red Hat Enterprise Linux Server 10.x.
- Агент администрирования теперь поддерживает работу со следующими новыми версиями операционных систем:
  - Альт Рабочая станция 11.
  - Альт Сервер 11.
  - Альт Образование 11.
  - AlterOS 2025.
  - SberOS 3.4.0.
  - SberOS 3.5.0.
  - ОСнова 3.*.

Kaspersky Security Center 16 Linux

В приложении Kaspersky Security Center 16 Linux реализовано несколько новых функций и улучшений:

- Поддерживаются контроллеры домена FreeIPA и ALD Pro.
- Реализована доменная аутентификация (единый вход). Функция единого входа позволяет вам включить безопасную аутентификацию в Kaspersky Security Center 16 Web Console без повторного ввода пароля в корпоративной сети. Чтобы использовать доменную аутентификацию, вам нужно указать дополнительные параметры в файле ответов при установке Kaspersky Security Center Web Console.
- Сервер администрирования Kaspersky Security Center 16 Linux совместим только с Kaspersky Security Center 16 Web Console. Более ранние версии Kaspersky Security Center Web Console использовать невозможно.

- Теперь вы можете использовать функциональность Kaspersky Security для бизнеса Профессиональный по пробной лицензии при условии, что вы добавили подчиненный Сервер администрирования, активировали этот Сервер по пробной лицензии и распространили лицензионный ключ на устройства, управляемые подчиненным Сервером администрирования.

- Улучшен пользовательский опыт:

  - Обновлена навигация по группам администрирования и Серверам администрирования: вы можете легко переключаться между группами и Серверами из единой панели навигации.

  - Параметры вашего профиля перенесены в верхнюю панель.

  - Следующие разделы главного меню переименованы:

    - Раздел **Активы (Устройства)** теперь называется **Управление активами**.

    - Раздел **Управляемые устройства** теперь называется **Управляемые устройства**.

    - Раздел **Быстрые ссылки** теперь называется **Навигация консоли**.

  - При необходимости вы можете свернуть главное меню до значков.

  - Раздел **Корпоративные новости "Лаборатории Касперского"** удален из **Мониторинг → Уведомления**.

- Фильтры, которые вы применяете к таблицам в разделах **Операции → Управление патчами → Уязвимости в приложениях** и **Операции → Управление патчами → Обновления ПО**, теперь успешно сохраняются и не сбрасываются.

- Kaspersky Security Center Linux поддерживает работу:

  - С Kaspersky NGFW.

  - Со следующими версиями операционной системы (для управляемых устройств):

    - МосОС 15.5 Arbat.

    - Microsoft Windows 11 25H2.

    - CentOS 6.4.

    - CentOS 6.6.

Kaspersky Security Center 15.4 Linux

В приложении Kaspersky Security Center 15.4 Linux реализовано несколько новых функций и улучшений:

- Теперь доступны профили соединения для автономных пользователей с Linux-устройствами. Используя профили соединения, вы можете настроить правила для Агентов администрирования на Linux-устройствах для подключения к одному и тому же или разным Серверам администрирования в зависимости от местоположения устройства.

- Теперь доступна передача ключей шифрования между Серверами администрирования.

- Теперь поддерживается Kaspersky Thin Client.
- Теперь поддерживается Platform V Pangolin кластер Built-in High Availability.
- Теперь поддерживается кластер Postgres Pro Built-in High Availability. Узлы этого кластера СУБД нужно указать в строке подключения при установке Kaspersky Security Center Linux.
- Kaspersky Security Center Linux теперь поддерживает работу со следующими СУБД:
  - Platform V Pangolin 6.5.1.
  - Tantor SE 1C для Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8).
  - Jatoba 5.
- Поддержка Platform V SberLinux OS Server (SLO) версий 8.10.1, 9.0.1, 9.5.1.
- Архив KlAkOAPI.tar.gz удален из справки. Архив KlAkOAPI.tar.gz находится в папке установки Kaspersky Security Center Linux.
- Кнопка **Проверка** удалена из раздела **Карантин**.
- Информация о размере файла, хеше файла и пути больше недоступна в списке инсталляционных пакетов для автономного пакета Агента администрирования, а также для пакетов, созданных на виртуальных Серверах администрирования, поскольку эти автономные пакеты генерируются во время загрузки.

Активация Kaspersky Security Center 15.4 Linux по лицензии Kaspersky Security для бизнеса Профессиональный

Если вы активировали Сервер администрирования по лицензии Kaspersky Security для бизнеса Профессиональный и распространили лицензионный ключ Kaspersky Security для бизнеса Профессиональный на управляемые приложения, вы можете выполнять следующее:

- Группировать алерты по атрибутам.
- Настраивать интеграцию для реагирования на угрозы.

Kaspersky Security Center 15.3 Linux

В приложении Kaspersky Security Center 15.3 Linux реализовано несколько новых функций и улучшений:

- Утилита klcsngtgui удалена из комплекта поставки Kaspersky Security Center Linux. Рекомендуется использовать утилиту klnagchk вместо утилиты klcsngtgui.
- Агент администрирования теперь поддерживает работу со следующими новыми версиями операционных систем:
  - Windows Server 2025.
  - Fedora Linux Server 41.
  - Fedora Linux Workstation 41.

- Kaspersky Security Center Linux теперь поддерживает работу со следующими СУБД:
  - PostgreSQL 17.
  - Postgres Pro 17.
- Теперь вы можете загружать только необходимые обновления баз данных и модулей приложений для приложений безопасности "Лаборатории Касперского" с помощью утилиты Kaspersky Update Utility. В окне свойств задачи **Загрузка обновлений в хранилище Сервера администрирования** включите параметр **Скачать файл запроса на обновление автоматически** и укажите путь, по которому Kaspersky Security Center Linux создаст файл запроса на обновление с информацией о загружаемых обновлениях.
- Теперь доступен просмотр статистики использования прокси-сервера KSN.
- Обновлен перенос данных Сервера администрирования Kaspersky Security Center Windows на Kaspersky Security Center Linux с использованием утилиты klbackup. Теперь вы можете переносить данные Сервера администрирования, хранящиеся в базе Microsoft SQL Server, в PostgreSQL или Postgres Pro.
- Теперь доступна настройка адреса подключения к Серверу администрирования. Адрес подключения к Серверу администрирования используется как адрес по умолчанию при создании инсталляционных пакетов Агента администрирования и как адрес прокси-сервера KSN при подключении управляемых устройств к KSN.
- Теперь вы можете централизованно перезагружать управляемые устройства.
- Информация о пользователях, в настоящее время вошедших в систему на управляемом устройстве Linux, теперь отображается в окне свойств устройства в разделе **Общие** → **Сеансы**.
- Теперь вы можете получать удаленный доступ к управляемым устройствам Linux и Windows с помощью Агента администрирования, установленного на этих устройствах. Подключение устанавливается с использованием RDP, VNC или WDS. После подключения к устройству администратор получает полный доступ к информации на этом устройстве и может управлять приложениями, установленными на нем.
- Загрузите и запустите приложение (или скрипт) для диагностики на управляемом устройстве. Теперь вы можете загрузить либо директорию или архив, содержащий исполняемый файл, либо сам исполняемый файл. После успешного выполнения приложения, вы можете скачать результаты выполнения.
- Улучшен пользовательский опыт, включая новый раздел **Быстрые ссылки**. Этот раздел отображает карту главного меню и обеспечивает вам быстрый доступ ко всем разделам Kaspersky Security Center Web Console. Раздел **Быстрые ссылки** установлен как домашняя страница по умолчанию.

Kaspersky Security Center 15.2 Linux

В приложении Kaspersky Security Center 15.2 Linux реализовано несколько новых функций и улучшений:

- Новые функции управления паролями внутренних учетных записей пользователей:
  - Теперь вы можете принудительно сменить пароль при первой (или следующей) попытке входа внутреннего пользователя в Kaspersky Security Center Web Console.
  - Новый параметр для настройки срока действия пароля для учетных записей внутренних пользователей.

- Теперь вы можете создать резервную копию данных Сервера администрирования Kaspersky Security Center Windows и восстановить их в Kaspersky Security Center Linux с помощью утилиты klbackup. Перенос данных возможен без потери данных между СУБД одного типа, Microsoft SQL Server → MySQL или MariaDB.
- Kaspersky Security Center Linux теперь поддерживает работу со следующими СУБД:
  - PostgreSQL 16.x.
  - Postgres Pro 16.x.
- Kaspersky Security Center Linux теперь поддерживает некоторые типы кластеров PostgreSQL и Postgres Pro.
- Поддержка новых операционных систем и новых версий операционных систем, включая новые версии ОС МЭШ (Moscow Electronic School), МосТех и МосТех Сервер.
- Улучшен пользовательский опыт при использовании приложения, в том числе:
  - Новая кнопка **Сохранить** в окне свойств политики. Используйте эту кнопку, если вы хотите сохранить изменения, не закрывая окно параметров политики.
- Теперь вы можете управлять загрузкой файлов на Android-устройства, удалять ранее загруженные файлы, а также настраивать их параметры в новом разделе плагина Kaspersky Mobile Devices Protection and Management "Приложения и файлы".
- Теперь вы можете передавать устройствам инсталляционные пакеты приложений и управляющие профили без прямого подключения устройств к Серверу администрирования с помощью новой службы Веб-сервера на шлюзе соединения.

Kaspersky Security Center 15.1 Linux

В приложении Kaspersky Security Center 15.1 Linux реализовано несколько новых функций и улучшений:

- Kaspersky Security Center Web Console теперь поддерживает управление мобильными устройствами с помощью плагина Kaspersky Mobile Devices Protection and Management.
- Теперь вы можете установить и настроить Серверы iOS MDM с помощью плагина параметров Сервера iOS MDM для управления iOS MDM-устройствами.
- Теперь вы можете управлять сертификатами мобильных устройств.
- Поддерживается Kaspersky Endpoint Security для Android.
- Поддерживается Kaspersky Security для iOS.
- Поддерживается Kaspersky Endpoint Security для ОС Аврора.
- Системное администрирование для управляемых устройств с операционной системой Windows. Вы можете управлять обновлениями стороннего программного обеспечения, установленного на управляемых устройствах с операционными системами Windows, и закрывать уязвимости в таких приложениях путем установки требуемых обновлений.

- Kaspersky Security Center Linux теперь опрашивает контроллеры домена постранично, а не сразу весь контроллер домена. Это позволяет опрашивать контроллеры домена, содержащие большое количество записей.

- Адаптивный контроль аномалий. Эта функция Kaspersky Endpoint Security для Windows, которая использует набор правил для отслеживания нестандартного поведения на клиентских устройствах и позволяет блокировать аномальные действия.

- Обновления для управляемых приложений "Лаборатории Касперского", установленных на устройствах под управлением Windows, и Агента администрирования для Linux. Вы можете управлять процессом установки обновлений, одобряя обновления, которые должны быть установлены, и отклоняя обновления, которые не должны быть установлены.

- Расширенный аудит политик. Теперь вы можете просмотреть ревизию политики и сохранить ревизию политики в файл. В настоящее время эти возможности доступны только для политики Сервера администрирования и Агента администрирования.

- Cloud Discovery. Новая функциональность приложения Kaspersky Security Center Linux позволяет отслеживать использование облачных сервисов на управляемых устройствах с операционной системой Windows и блокировать доступ к нежелательным облачным сервисам.

- Новый подраздел **Алерты** в разделе **Мониторинг** главного меню. В разделе **Алерты** вы можете просматривать информацию об обнаруженных угрозах на устройствах. Угрозы обнаруживаются приложениями безопасности "Лаборатории Касперского".

- Kaspersky Security Center Linux теперь является компонентом решения Kaspersky Managed Detection and Response.

- Поддерживается Kaspersky Security для виртуальных сред Легкий агент.

- Расширенная инвентаризация macOS-устройств. Агент администрирования на macOS-устройстве отправляет MAC-адрес и серийный номер устройства на Сервер администрирования.

- Теперь вы можете получать отчет об удаленной установке при установке программного обеспечения на управляемые устройства с помощью пользовательских скриптов.

- При выполнении нескольких пользовательских скриптов на управляемом устройстве, вы можете установить приоритет для каждого скрипта, чтобы определить порядок их выполнения. Скрипты будут выполняться от скрипта с наивысшим приоритетом к скрипту с наименьшим приоритетом.

- Чтобы уменьшить объем оперативной памяти, потребляемой Kaspersky Endpoint Security для Linux и Агентом администрирования для Linux, вы можете включить специальный режим работы Агента администрирования для Linux. В этом режиме Агент администрирования для Linux требует меньше оперативной памяти, но его функциональность ограничена.

- Вы можете удалить несовместимое программное обеспечение с управляемых устройств с помощью задачи *Удаленная деинсталляция приложения*.

- Отчет о сетевых атаках теперь включает MAC-адрес и порт атакующего устройства.

- Максимальная длина пароля для внутреннего пользователя увеличена до 256 символов.

- Улучшен пользовательский опыт при использовании приложения, в том числе:
  - Персонализация главного меню путем добавления разделов Kaspersky Security Center Web Console в закладки для быстрого доступа из раздела **Закладки**.
  - Оптимизирована работа с таблицами. Представление по умолчанию для каждой таблицы теперь содержит наиболее часто используемые столбцы. Также теперь вы можете выбрать все элементы на текущей странице или во всей таблице и отсортировать элементы по всей таблице.
  - Улучшена конфигурация рассылки отчетов. Теперь вы можете указать до 20 адресов электронной почты для рассылки отчета и задать расписание рассылки отчета.
- Поддержка широкого спектра операционных систем и новых версий операционных систем.
- Новое руководство по масштабированию было разработано и опубликовано в справке.
- В результате анализа пользовательского интерфейса была решена проблема, приводившая к появлению раздела **Удаленная диагностика** в окне свойств Сервера администрирования.
- Вы можете создать задачу *Удаленное выполнение скриптов* для выполнения инсталляционного пакета на клиентском устройстве и удаленной установки приложения.
- Пользователь может быть назначен владельцем устройства во время или после установки Агента администрирования на клиентском устройстве под управлением Linux.
- Вы можете настроить выборку устройств или создать правило перемещения устройств на основе владельца устройства, членства владельца устройства в группе безопасности и роли владельца устройства.
- Вы можете отозвать права локального администратора для учетных записей. Это дает вам дополнительный уровень контроля учетных записей пользователей. Например, вы можете отозвать права локального администратора после завершения разового назначения.
- Вы можете изменить пароль локальной учетной записи, например, когда пользователь забыл пароль локальной учетной записи или чтобы изменить пароль по расписанию.
- В подразделе **Управление пользовательскими сертификатами** вы можете указать, какие корневые сертификаты устанавливать. Эти сертификаты могут использоваться, например, для проверки подлинности веб-сайтов или веб-серверов.

Kaspersky Security Center 15 Linux

В приложении Kaspersky Security Center 15 Linux реализовано несколько новых функций и улучшений:

- Опрос контроллеров домена, который позволяет опрашивать контроллер домена Microsoft Active Directory и контроллер домена Samba. Вы можете использовать Сервер администрирования или точку распространения для опроса Microsoft Active Directory. Вы можете опрашивать контроллеры домена Samba только с помощью точки распространения с операционной системой Linux. При опросе контроллера домена Сервер администрирования или точка распространения получают информацию о структуре домена, учетных записях пользователей, группах безопасности и о DNS-именах устройств, входящих в домен.

- Kaspersky Security Center Linux теперь поддерживает работу со следующими СУБД:

  - PostgreSQL 15.x.

  - Postgres Pro 15.x.

- Если вы используете PostgreSQL или Postgres Pro в качестве СУБД, Kaspersky Security Center Linux поддерживает до 50 000 управляемых устройств.

- Перенос данных из Kaspersky Security Center Windows в Kaspersky Security Center Linux. Вы можете запустить мастер переноса данных объектов Kaspersky Security Center, включая задачи, политики и структуру групп администрирования. После этого вы можете переместить импортированные управляемые устройства под управление Kaspersky Security Center Linux.

- Kaspersky Security Center Linux теперь поддерживает работу со следующими приложениями "Лаборатории Касперского":

  - Kaspersky Security для виртуальных сред Легкий агент

  - Kaspersky Embedded Systems Security для Windows

  - Kaspersky Embedded Systems Security для Linux

  - Kaspersky Industrial CyberSecurity for Nodes

  - Kaspersky Industrial CyberSecurity for Networks

  - Kaspersky Endpoint Security для Mac

  - Kaspersky Endpoint Agent

  - Kaspersky Security для виртуальных сред Легкий агент

- Удаленная диагностика управляемых устройств с операционными системами Windows и Linux.

- Улучшенный компонент Контроль приложений. Вы можете создать категорию приложений на основе списка исполняемых файлов из выбранной папки или на основе категории для приложений "Лаборатории Касперского". Затем можно указать, хотите ли вы разрешить или запретить приложения из созданной категории в своей организации.

- Экспорт и импорт выборок событий. Вы можете экспортировать определенную пользователем выборку событий и ее параметры в файл KLO, а затем импортировать сохраненную выборку событий в Kaspersky Security Center Windows или Kaspersky Security Center Linux.

- В отчете об угрозах теперь можно открыть цепочку развития угроз, перейдя по ссылке **Просмотреть алерт**.

- Kaspersky Security Center Linux теперь поддерживает кластерную технологию. Если группа администрирования содержит кластеры или массивы серверов, на странице **Управляемые устройства** отображаются две вкладки: одна для отдельных устройств, другая для кластеров и массивов серверов. После обнаружения управляемых устройств в качестве узлов кластера, кластер добавляется как отдельный объект на вкладку **Кластеры и массивы серверов**. Узлы кластера перечислены на вкладке **Устройства** вместе с другими управляемыми устройствами.

- Поддержка некоторых платформ приложением Kaspersky Security Center Linux прекращена, так как эти платформы больше не поддерживаются их поставщиками.

Kaspersky Security Center 14.2 Linux

В приложении Kaspersky Security Center 14.2 Linux реализовано несколько новых функций и улучшений:

- В иерархия Серверов администрирования Сервер администрирования с операционной системой Linux теперь может выступать в качестве главного Сервера и может управлять Серверами с операционными системами Linux или Windows в качестве подчиненных.

- Kaspersky Security Center Linux теперь поддерживает Kaspersky Security Network (KSN), службу прокси-сервера KSN и Kaspersky Private Security Network (KPSN).

- Kaspersky Security Center Linux теперь поддерживает Kaspersky Endpoint Security для Windows как управляемое приложение.

  Удаленная установка Агента администрирования с операционной системой Windows на клиентские устройства возможна только средствами операционной системы точки распространения с операционной системой Windows.

- Шифрование данных устройств с операционной системой Windows снижает риски непреднамеренной утечки информации в случае кражи/утери портативного устройства или жесткого диска. Эта функциональность реализована через Kaspersky Endpoint Security для Windows.

- Kaspersky Security Center Linux позволяет загружать и обновлять дистрибутивы приложений "Лаборатории Касперского" и веб-плагины управления в пользовательском интерфейсе Kaspersky Security Center Linux.

- По умолчанию информация о приложениях, установленных на управляемых устройствах под управлением Linux и Windows, передается на Сервер администрирования.

- Доступ к серверам "Лаборатории Касперского" теперь проверяется автоматически. Если доступ к серверам через системный DNS невозможен, приложение использует публичный DNS.

- Конфиденциальные данные, передаваемые между главным Сервером администрирования, подчиненными Серверами администрирования и Агентами администрирования, теперь защищены алгоритмом шифрования AES.

- Права пользователя виртуального Сервера администрирования настраиваются независимо от прав пользователей главного Сервера администрирования. Также вы можете предоставить пользователям главного Сервера права на управление виртуальным Сервером.
- Kaspersky Security Center Linux теперь поддерживает работу со следующими СУБД:
  - PostgreSQL 13.x.
  - PostgreSQL 14.x.
  - Postgres Pro 13.x (все редакции).
  - Postgres Pro 14.x (все редакции).
- Вы можете использовать Kaspersky Security Center Web Console для экспорта политик и задач в файл, а затем импортировать политики и задачи в Kaspersky Security Center Windows или Kaspersky Security Center Linux.
- Параметр **Не использовать прокси-сервер** удален из следующих задач:
  - *Загрузка обновлений в хранилище Сервера администрирования*
  - *Загрузка обновлений в хранилища точек распространения*

Kaspersky Security Center 14 Linux

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

- Кроме задачи *Загрузка обновлений в хранилище Сервера администрирования*, антивирусные базы для приложений безопасности "Лаборатории Касперского" теперь можно загружать с помощью задачи *Загрузка обновлений в хранилища точек распространения*.
- Антивирусные базы и модули приложений 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 Linux загружает с серверов обновлений "Лаборатории Касперского" только те обновления, которые запрашиваются приложениями безопасности "Лаборатории Касперского". Это уменьшает размер загружаемых данных.
- Теперь вы можете использовать функцию файлов различий, чтобы загружать антивирусные базы и модули приложений. Файл различий описывает различия между двумя версиями файлов базы или модулями приложения. Использование файлов различий сохраняет трафик внутри сети вашей организации, так как файлы различий занимают меньше места, чем целые файлы баз и модулей приложений.
- 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 Linux теперь поддерживает Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 как управляемое приложение.

Исправленные ошибки

В таблице ниже перечислены все проблемы, обнаруженные в предыдущих версиях Kaspersky Security Center Linux и исправленные в текущей версии.

Список проблем, исправленных в Kaspersky Security Center Linux 17

Версия Kaspersky Security Center Linux, в которой проблема появилась впервые	Идентификатор проблемы	Описание проблемы
16.2	10575601	Исправлена проблема, при которой при создании правила перемещения после включения параметра **Устройство находится в подгруппе группы "Домены"** в выпадающем списке не отображался список групп.
16.3	10519188	Исправлена проблема, при которой вакуумирование (`VACUUM`) временных таблиц приводило к замедлению работы Сервера администрирования.
16.3	10530831	Исправлена проблема, при которой в разделе **Управляемые устройства** после изменения порядка столбцов изменения не сохранялись.
16.3	10698217	Исправлена проблема, при которой в свойствах управляемого устройства на вкладке **Дополнительно → Удаленная диагностика → Журналы событий** при переходе по ссылке **Журналы удаленной установки** открывшееся окно называлось **Журналы удаленной установки**.
16.3	10696918	Исправлена проблема, при которой на подчиненном Сервере в разделе **Сторонние приложения → Категории приложений** при переходе в свойства категории на вкладке **Условия** не открывалось окно поиска.
16.3	10720529	Исправлена проблема, при которой в таблице управляемых устройств в фильтре **Последнее подключение к Серверу администрирования** при использовании оператора "≠" (не равно) некорректно отображались данные.
16.3	10012561	Исправлена проблема, при которой сканирование домена с помощью SberLDAP не возвращало структуру домена и его хостов.
16	9496192	Исправлена проблема, при которой по нажатию на кнопку **Выбрать все** в таблице **Выборка событий** и последующем экспорте экспортировались события только с текущей страницы.
16.3	10292104	Исправлена проблема, при которой в Kaspersky Security Center Web Console версии 15.1 или 15.2 при обновлении плагина Kaspersky Endpoint Detection and Response Optimum до версии 16.3 в разделе **Алерты** могли не отображаться алерты.
16.3	10596319	Исправлена проблема, при которой в разделе **Теги** в форме **Назначить тег** список тегов отображался в неотсортированном виде.
16.3	10127434	Исправлена проблема, при которой после входа в Kaspersky Security Center Web Console и перехода в раздел **Задачи** на главном Сервере администрирования в окне иерархии виртуальный Сервер администрирования отображался как главный.
16.3	10252324	Исправлена проблема, при которой не все приложения из выборки событий, генерируемых компонентом **Контроль приложений** в политике Kaspersky Endpoint Security, попадали в раздел **Категории приложений**.
16.3	10308380	Исправлена проблема, при которой после создания категории приложений не открывались ее свойства.
16.2	10698205	Исправлена проблема, при которой не отображался раздел **Кластеры и массивы серверов** при выборе кластера в разделе **Управляемые устройства**, из-за чего перемещение кластера в группу было недоступно.
16.3	10373324	Исправлена проблема, при которой второй узел отказоустойчивого кластера Kaspersky Security Center Linux не учитывался при расчете статуса индикатора защищенности.

16.3	10563031	Исправлена проблема, при которой обновление отказоустойчивого кластера Kaspersky Security Center Linux с версии 16.2 до версии 16.3 и с версии 16 до версии 16.3 приводило к ошибке "Attempt to change KLFOC-mode in upgrade. Aborting".
16.3	10590796, 10590805	Исправлена проблема, при которой обновление вторичного узла отказоустойчивого кластера Kaspersky Security Center Linux приводило к ошибкам "Fatal error: It is forbidden to change KLFOC-management mode!" и "Fatal error: Can't get KSC DB name from settings storage."
16.3	10570574	Исправлена проблема, при которой перезапуск службы Сервера администрирования во время работы задачи **Резервное копирование данных Сервера администрирования** приводил к тому, что повторный запуск задачи завершался с ошибкой "Резервное копирование уже выполняется".
16.3	10085767	Исправлена проблема, при которой при переносе данных в Kaspersky Security Center Linux область действия отчета могла отображаться некорректно.
16.2	10135898	Исправлена проблема, при которой раздел **Настройки** → **Единый вход** не загружался, если пользовательская сессия длилась более часа.
16.3	10542356	Исправлена ошибочная валидация поля **Адрес электронной почты** при редактировании пользователя в разделе **Пользователи и роли** → **Пользователи и группы**.
16.3	10534809	Исправлена проблема, при которой события управляемого устройства долго загружались. Время загрузки сокращено с 20 до 2 секунд.
16.3	10537996	Исправлена проблема, при которой вкладка с Kaspersky Security Center Web Console потребляла более 1,5 ГБ ОЗУ в браузере.
15.1	9067495	Исправлена проблема, при которой кнопка **Проверить подключение** была доступна при сохранении настроек подключения к SIEM с протоколом UDP.

Список проблем, исправленных в Kaspersky Security Center Linux 16.3 Update 1

Версия Kaspersky Security Center Linux, в которой проблема появилась впервые	Идентификатор проблемы	Описание проблемы
16.3	10431901	Исправлена проблема, из-за которой в меню Web Console отсутствовал раздел **Единый вход**. Из-за этого пользователи не могли настроить доменную аутентификацию по протоколу Kerberos. Ранее настроенная аутентификация продолжала работать.

Список проблем, исправленных в Kaspersky Security Center Linux 16.3

Версия Kaspersky Security Center Linux, в которой проблема появилась впервые	Идентификатор проблемы	Описание проблемы
16.2	9959974	Исправлена ошибка, из-за которой на вкладке **События** окна свойств устройства присутствовал параметр **Выбрать все**, при выборе которого могли быть удалены все события из базы данных Сервера администрирования.
16.2	9392997	Исправлена ошибка, из-за которой в журнал событий добавлялось сообщение об ошибке после успешного опроса контроллера домена ALD Pro или FreeIPA.
16.2	9504495	Исправлена ошибка, которая могла привести к неправильному назначению пользователя, если владелец устройства был назначен в параметрах инсталляционного пакета Агента администрирования.
16.1	9316206	Исправлена ошибка, из-за которой кнопки управления могли исчезать с вкладки **Двухфакторная аутентификация** при обновлении браузера после открытия вкладки.

16.1	7555541	Исправлена ошибка, из-за которой не удавалось войти в Web Console, если параметр **Установить в качестве одноразового пароля (пользователь должен изменить пароль после первого входа в систему)** был включен при создании задачи *Изменить пароль учетной записи (только для Linux).*
15.4	7555788	Исправлена ошибка, из-за которой задача *Изменить пароль учетной записи* могла работать некорректно, если на устройстве пользователя был включен SELinux.
16.2	9603496	Исправлена ошибка, из-за которой на устройстве Сервера администрирования требовалось установить Агент администрирования для получения диагностической информации об этом устройстве.
16.2	9704308	Исправлена ошибка, из-за которой при открытии раздела **Иерархия групп** администрирования во время загрузки страницы в средах с большим количеством групп администрирования могло привести к ошибке `429 Too Many Requests` и могло прерываться подключение к Серверу администрирования и пользователей перенаправляло на страницу входа в приложение.
16.2	9989231	Исправлена ошибка, из-за которой фильтрация устройств по IP-адресу подключения могла возвращать неверные результаты.
16.2	9990025	Исправлена ошибка, из-за которой параметры табличного представления в разделах **Политики** и **Задачи** не сохранялись при переходе между страницами.
15.3	9632613	Исправлена ошибка, из-за которой вход доменного пользователя в Web Console мог значительно задерживаться, когда контроллеры домена LDAP были недоступны или не содержали учетную запись пользователя.
15.1	9829027	Исправлена ошибка, из-за которой настройка фильтра **Статус антивирусных баз** в отчете **Отчет об используемых антивирусных базах** могла привести к ошибке.
15.1	9844707	Kaspersky Security Center и FCM (Firebase Cloud Messaging) взаимодействовали напрямую, даже если был настроен прокси-сервер.

Список проблем, исправленных в Kaspersky Security Center Linux 16.2

Версия Kaspersky Security Center Linux, в которой проблема появилась впервые	Идентификатор проблемы	Описание проблемы
15.1	10071566	Исправлена ошибка, из-за которой изменения, внесенные в расписание задачи, не распространялись на управляемые устройства, если в расписании использовался параметр "По дням недели".
15.4	9067754	Исправлена ошибка, из-за которой новые события некорректно отображались в ранее созданной политике после обновления плагина Kaspersky Mobile Devices Protection and Management.
16	9329729	Исправлена ошибка, из-за которой в журнале Kaspersky Event Log после обновления Kaspersky Security Center Linux с версии 16 до версии 16.1 была настроена двухфакторная аутентификация для определенных пользователей перед обновлением.
16.1	9256000	Исправлена ошибка, из-за которой информация о компонентах управляемых приложений была недоступна, если Агент администрирования установлен на устройстве с операционной системой Microsoft Windows XP.
16.1	9251629	Исправлена ошибка, из-за которой некоторые обязательные заголовки HTTP-ответов не добавлялись при входе в Kaspersky Security Center Web Console.

О Kaspersky Security Center Linux

В этом разделе представлена информация о назначении, ключевых возможностях и компонентах приложения 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 клиентских устройств с помощью Сервера администрирования на базе Linux.

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

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

Приложение Kaspersky Security Center Linux адресовано администраторам сетей организаций и сотрудникам, отвечающим за защиту устройств в организациях.

При помощи Kaspersky Security Center вы можете:

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

  Под *организациями-клиентами* здесь подразумеваются организации, антивирусную защиту которых обеспечивает поставщик услуг.

- Формировать иерархию групп администрирования для управления набором клиентских устройств как единым целым.

- Управлять системой антивирусной безопасности, построенной на основе приложений "Лаборатории Касперского".

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

- Централизованно распространять лицензионные ключи приложений "Лаборатории Касперского" на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.

- Получать статистику и отчеты о работе приложений и устройств.

- Получать уведомления о критических событиях в работе приложений "Лаборатории Касперского".

- Управлять шифрованием данных, хранящихся на жестких дисках устройств с операционной системой Windows и съемных дисках.

- Управлять доступом пользователей к зашифрованным данным устройств с операционной системой Windows.

- Проводить инвентаризацию оборудования, подключенного к сети организации.

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

Вы можете приобрести Kaspersky Security Center Linux 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 приложение с нашего сайта. Информация, необходимая для активации приложения, 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 приложении на территории США.

Комплект поставки

На сайте "Лаборатории Касперского", вы можете скачать все необходимые дистрибутивы приложения.

В состав дистрибутива Kaspersky Security Center Linux входят следующие файлы:

Сервер администрирования Kaspersky Security Center Linux:

- Сервер администрирования для установки на устройстве с операционной системой на базе Debian:

  ksc64_17.0.0-<build>_amd64.deb

- Сервер администрирования для установки на устройстве с операционной системой на базе Red Hat Enterprise Linux:

  ksc64-17.0.0-<build>.x86_64.rpm

Kaspersky Security Center Web Console:

- Приложение Web Console для установки на устройстве с операционной системой на базе Debian:

  ksc-web-console-17.0.<build>.x86_64.deb

- Приложение Web Console для установки на устройстве с операционной системой на базе Red Hat Enterprise Linux:

  ksc-web-console-17.0.<build>.x86_64.rpm

Установочный скрипт Kaspersky Security Center:

- ksc_fast_install.tar.gz

Агент администрирования для Windows:

- Агент администрирования для установки на устройство с архитектурой Arm:

  klnagent_winarm64-17.0.0.<build>-win_<localization>.zip

- Файлы для удаленной установки Агента администрирования на устройство с архитектурой x86-32 или x64:

  ksc_17_17.0.0.<build>_NetAgent_<localization>.zip

- Файлы для удаленной установки Агента администрирования на устройство с архитектурой Arm:

  ksc_17_17.0.0.<build>_NetAgent_arm64_<localization>.zip

- Файлы для удаленной установки с помощью Kaspersky Security Center на устройство с архитектурой Arm:

  ri_utils_arm64.zip

- Файлы для удаленной установки с помощью Kaspersky Security Center на устройство с архитектурой x86-32 или x64:

  ri_utils_win32.zip

Агент администрирования для Linux:

- Агент администрирования для установки на устройстве с операционной системой на базе Debian:

  klnagent64_17.0.0-<build>_<architecture>.deb

- Агент администрирования для установки на устройстве с операционной системой на базе Red Hat Enterprise Linux:

  klnagent64-17.0.0-<build>_<architecture>.rpm

- Файлы для удаленной установки Агента администрирования на устройстве с операционной системой на базе Debian:

  klnagent-<architecture>-17.0.0.<build>-deb_<localization>.tar.gz

- Файлы для удаленной установки Агента администрирования на устройстве с операционной системой на базе Red Hat Enterprise Linux:

  klnagent-<architecture>-17.0.0.<build>-rpm_<localization>.tar.gz

- Файлы для удаленной установки Агента администрирования Elbrus Edition на устройстве с операционной системой на базе Debian или Red Hat Enterprise Linux:

  klnagent-e2k-17.0.0.<build>-all-<localization>.tar.gz

- Единый дистрибутив для удаленной установки Агентов администрирования для Linux:

  klnagent-all-17.0.0.<build>-all_<localization>.tar.gz

  Единый дистрибутив может быть полезен, если у вас много клиентских устройств с разной архитектурой процессора и различные операционные системы на базе Linux. Необходимые версии Агентов администрирования будут автоматически выбраны для дальнейшей установки на устройства.

- Файлы для удаленной установки Агента администрирования на устройство с устаревшими операционными системами на базе Debian или Red Hat Enterprise Linux с glibc 2.5:

  klnagent-all-17.0.0.<build>-glibc2.5-all-<localization>.tar.gz

Веб-плагин Kaspersky Endpoint Detection and Response Optimum:

- signed_irp.zip

  Вы можете загрузить веб-плагин только из хранилища дистрибутивов приложений для удаленной установки.

Если вы затрудняетесь выбрать инсталляционный пакет Агента администрирования для Linux, см. статью Как выбрать инсталляционный пакет Агента администрирования для Linux.

Аппаратные и программные требования

- Требования Сервера администрирования
- Требования Web Console
- Требования Агента администрирования

Требования к версиям Android и iOS для развертывания защиты и управления мобильными устройствами см. в справке Kaspersky Security для мобильных устройств и справке Kaspersky Secure Mobility Management.

Требования Сервера администрирования

В этой статье указаны версии программного обеспечения, на которых приложение было протестировано и для которых гарантируется его корректная работа. Приложение также может работать с другими версиями программного обеспечения, но такие конфигурации не проходили полного цикла тестирования и не входят в список гарантированно поддерживаемых.

Минимальные аппаратные требования:

- Процессор с частотой 2,5 ГГц или выше, 2 ядра.
- Оперативная память: 6 ГБ.

  Необходимо включить файл подкачки на устройстве с установленным Сервером администрирования. Минимальный размер файла подкачки должен быть в 1,5 раза больше объема оперативной памяти.
- Объем свободного места на диске: требуется 10 ГБ для папки, где хранятся данные Сервера администрирования (/var/opt/kaspersky/klnagent_srv).

Дополнительные сведения об аппаратных требованиях см. в разделе Аппаратные требования к СУБД и Серверу администрирования.

После установки Сервера администрирования на устройство рекомендуется установить Kaspersky Endpoint Security для Linux.
Для совместной установки у вас должно быть не менее 300 IOPS, а также нужно добавить к требованиям Сервера администрирования 1,5 ГБ ОЗУ и 15% к требованиям процессора.
Требования к оборудованию для Kaspersky Endpoint Security см. в справке Kaspersky Endpoint Security для Linux.
Информацию о параметрах безопасности, необходимых для работы с Kaspersky Security Center Linux, см. в справке Kaspersky Endpoint Security для Linux.

Поддерживаются следующие операционные системы:

Для межпроцессного взаимодействия в операционной системе необходим доступ к интерфейсу обратной связи (loopback).

- Debian GNU/Linux 12.0, 12.1, 12.2, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 12.13 (Bookworm) 64-разрядная.
- Debian GNU/Linux 13.0, 13.1, 13.2, 13.3 (Trixie) 64-разрядная.
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная.
- Ubuntu Server 24.04 LTS (Noble Numbat) 64-разрядная.
- Ubuntu Server 26.04 LTS (Resolute Raccoon) 64-разрядная.
- CentOS Stream 9 64-разрядная.
- CentOS Stream 10 64-разрядная.
- Red Hat Enterprise Linux Server 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 64-разрядная.
- Red Hat Enterprise Linux Server 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 64-разрядная.
- Red Hat Enterprise Linux Server 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 64-разрядная.
- Red Hat Enterprise Linux Server 10.0, 10.1 64-разрядная.
- SUSE Linux Enterprise Server 12.5, 12.6, 12.7 64-разрядная.
- SUSE Linux Enterprise Server 15.0, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-17 (очередное обновление 1.7.3) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-03 (очередное обновление 7.6) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7) 64-разрядная.
- Astra Linux Common Edition (очередное обновление 2.12) 64-разрядная.
- Альт Сервер 11 64-разрядная.
- Альт СП Сервер 10 64-разрядная.
- Альт СП Рабочая станция 10 64-разрядная.
- Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 64-разрядная.

- Oracle Linux 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9 64-разрядная.
- Oracle Linux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 64-разрядная.
- Platform V SberLinux OS Server (SLO) 8.10.1 64-разрядная.
- Platform V SberLinux OS Server (SLO) 9.5.1 64-разрядная.
- Platform V SberLinux OS Server (SLO) 9.6 64-разрядная.
- Platform V SberLinux OS Server (SLO) 9.7 64-разрядная.
- РЕД ОС 7.3 Сервер 64-разрядная.
- РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.
- РЕД ОС 8 64-разрядная.
- РОСА "КОБАЛЬТ" 7.9 64-разрядная.
- M ОС (Moscow Electronic School) 12 Сервер 64-разрядная.
- МосТех Сервер 64-разрядная.
- МосОС Серверная 15.5 64-разрядная.
- МосОС Серверная 15.6 64-разрядная.

Рекомендуется использовать файловую систему EXT4 с параметрами по умолчанию.

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

- MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная.
- MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная.
- MySQL Standard Edition 8.4 32-разрядная/64-разрядная.
- MySQL Enterprise Edition 8.4 32-разрядная/64-разрядная.
- MariaDB 10.11 (сборка 10.11.10 и выше) 32-разрядная/64-разрядная.
- MariaDB 11.4 64-разрядная.
- MariaDB 11.8 64-разрядная.
- MariaDB 12.3 64-разрядная.
- MariaDB Galera Cluster 4 32-разрядная/64-разрядная.
- PostgreSQL 15.x 64-разрядная.
- PostgreSQL 15.x 64-разрядная (кластер Corosync/Pacemaker).

- PostgreSQL 16.x (все редакции) 64-разрядная.
- PostgreSQL 17.x (все редакции) 64-разрядная.
- PostgreSQL 18.x (все редакции) 64-разрядная.
- Postgres Pro 15.x (все редакции) 64-разрядная.
- Postgres Pro 15.x 64-разрядная (кластер Corosync/Pacemaker).
- Postgres Pro 16.x (все редакции) 64-разрядная.
- Postgres Pro 16.x Enterprise 64-разрядная (кластер Built-in High Availability).
- Postgres Pro 17.x (все редакции) 64-разрядная.
- Postgres Pro 17.x Enterprise 64-разрядная (кластер Built-in High Availability).
- Postgres Pro 18.x (все редакции) 64-разрядная.
- Postgres Pro 18.x Enterprise 64-разрядная (кластер Built-in High Availability).
- Platform V Pangolin 6.5.1 64-разрядная.
- Platform V Pangolin 6.5.1 64-разрядная (кластер Built-in High Availability).
- Platform V Pangolin 7.2.0 64-разрядная.
- Platform V Pangolin 7.2.0 64-разрядная (кластер Built-in High Availability).
- Jatoba 4 64-разрядная.
- Jatoba 5 64-разрядная.
- Tantor SE 1C 64-разрядная.

При использовании PostgreSQL и Postgres Pro версий 18.1-18.5 вы можете столкнуться с проблемой 10671377, описанной в статье Известные проблемы и ограничения.

Поддерживаются кластеры высокой надежности PostgreSQL. Подробнее см. в статье Подготовка кластера высокой доступности СУБД для работы с Kaspersky Security Center Linux.

Дополнительные сведения о поддерживаемых платформах виртуализации см. в справке Kaspersky Security для виртуальных сред Легкий агент.

Требования Web Console

В этой статье указаны версии программного обеспечения, на которых приложение было протестировано и для которых гарантируется его корректная работа. Приложение также может работать с другими версиями программного обеспечения, но такие конфигурации не проходили полного цикла тестирования и не входят в список гарантированно поддерживаемых.

Сервер Kaspersky Security Center Web Console

Минимальные аппаратные требования:

- Процессор: 2 ядра, частота от 2,5 ГГц.
- Оперативная память: 4 ГБ.
- Объем свободного места на диске: требуется 40 ГБ для папки, где хранятся данные Web Console (/var/opt/kaspersky).

После установки Kaspersky Security Center Web Console на устройство рекомендуется установить Kaspersky Endpoint Security для Linux. Аппаратные требования для Kaspersky Endpoint Security см. в справке Kaspersky Endpoint Security для Linux.

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

> Для межпроцессного взаимодействия в операционной системе необходим доступ к интерфейсу обратной связи (loopback).

- Debian GNU/Linux 12.0, 12.1, 12.2, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 12.13 (Bookworm).
- Debian GNU/Linux 13.0, 13.1, 13.2, 13.3 (Trixie).
- Ubuntu Server 22.04 LTS (Jammy Jellyfish).
- Ubuntu Server 24.04 LTS (Noble Numbat).
- Ubuntu Server 26.04 LTS (Resolute Raccoon).
- CentOS Stream 9.
- CentOS Stream 10.
- Red Hat Enterprise Linux Server 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
- Red Hat Enterprise Linux Server 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10.
- Red Hat Enterprise Linux Server 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6.
- Red Hat Enterprise Linux Server 10.0, 10.1.
- SUSE Linux Enterprise Server 12.5, 12.6, 12.7.
- SUSE Linux Enterprise Server 15.0, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).
- Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).

- Astra Linux Special Edition РУСБ.10015-17 (очередное обновление 1.7.3).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8).
- Astra Linux Special Edition РУСБ.10015-03 (обновление 7.6).
- Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7).
- Astra Linux Common Edition (очередное обновление 2.12).
- Альт Сервер 11.
- Альт СП Сервер 10.
- Альт СП Рабочая станция 10.
- Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
- Oracle Linux 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9.
- Oracle Linux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6.
- Platform V SberLinux OS Server (SLO) 8.10.1.
- Platform V SberLinux OS Server (SLO) 9.5.1.
- Platform V SberLinux OS Server (SLO) 9.6.
- Platform V SberLinux OS Server (SLO) 9.7.
- РЕД ОС 7.3 Сервер.
- РЕД ОС 7.3 Сертифицированная редакция.
- РЕД ОС 8.
- РОСА "КОБАЛЬТ" 7.9.
- М ОС (Moscow Electronic School) 12 Сервер.
- МосТех Сервер.
- МосОС Серверная 15.5.
- МосОС Серверная 15.6.

Дополнительные сведения о поддерживаемых платформах виртуализации см. в справке Kaspersky Security для виртуальных сред Легкий агент.

Клиентские устройства

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

Минимальное разрешение экрана составляет 1366x768 пикселей.

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

Браузеры:

- Google Chrome 154.0.8037.92.
- Microsoft Edge версии 154.0.4258.62.
- Safari 18.6 (20621.3.11.11.3) для macOS.
- Яндекс.Браузер версии 26.8.0.1788.
- Mozilla Firefox Extended Support Release версии 140.17.0.

Требования Агента администрирования

В этой статье указаны версии программного обеспечения, на которых приложение было протестировано и для которых гарантируется его корректная работа. Приложение также может работать с другими версиями программного обеспечения, но такие конфигурации не проходили полного цикла тестирования и не входят в список гарантированно поддерживаемых.

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.

Агент администрирования. Поддерживаемые платформы

Операционные системы. Рабочие станции Microsoft Windows	Microsoft Windows Embedded POSReady 2009 с последним Service Pack 32-разрядная. Microsoft Windows Embedded 7 Standard Service Pack 1 32-разрядная/64-разрядная. Microsoft Windows Embedded 8.1 Industry Pro 32-разрядная/64-разрядная. Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная/64-разрядная. Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная/64-разрядная. Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная/64-разрядная. Microsoft Windows 10 IoT Enterprise версия 1507, 1607, 1703, 1709, 1803, 1809, 1909 32-разрядная/64-разрядная. Microsoft Windows 10 20H2, 21H2 IoT Enterprise 32-разрядная/64-разрядная. Microsoft Windows 10 TH1 (July 2015) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 TH2 (November 2015) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 RS1 (August 2016) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 RS2 (April 2017) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 RS3 (Fall Creators Update, v1709) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 RS4 (April 2018 Update, 17134) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 RS5 (October 2018) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 RS6 (May 2019) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 19H1, 19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 20H1 (May 2020 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 20H2 (October 2020 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 21H1 (May 2021 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 21H2 (October 2021 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 10 22H2 (October 2023 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM 64-разрядная. Microsoft Windows 11 IoT Enterprise 25H2 64-разрядная. Microsoft Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная. Microsoft Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная. Microsoft Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная. Microsoft Windows 11 25H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная. Microsoft Windows 11 26H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная. Microsoft Windows 8.1 Pro/Enterprise 32-разрядная/64-разрядная. Microsoft Windows 8 Pro/Enterprise 32-разрядная/64-разрядная. Microsoft Windows 7 Professional/Enterprise/Ultimate/Home Basic/Premium Service Pack 1 и выше 32-разрядная/64-разрядная. Microsoft Windows XP Professional Service Pack 2 32-разрядная/64-разрядная (поддерживаются только для Агента администрирования обновленной версии 10.5.1781, которую вы можете запросить в Службе технической поддержки). Microsoft Windows XP Professional Service Pack 3 и выше 32-разрядная (поддерживается Агентом администрирования версии 14.0.0.20145, требуется Security Update for Windows XP KB2868626). Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32-разрядная (поддерживается Агентом администрирования версии 14.0.0.20145).

Операционные системы. Серверы Microsoft Windows	Microsoft Windows MultiPoint Server 2011 Standard/Premium 64-разрядная. Microsoft Windows Server 2003 SP1 32-разрядная/64-разрядная (поддерживаются только для Агента администрирования обновленной версии 10.5.1781). Microsoft Windows Server 2003 SP2 Standard/Enterprise 32-разрядная/64-разрядная (поддерживается Агентом администрирования обновленной версии 10.5.1781). Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 32-разрядная/64-разрядная (поддерживается Агентом администрирования обновленной версии 10.5.1781). Microsoft Windows Server 2008 R2 Datacenter/Enterprise/Foundation/Standard Service Pack 1 и выше 64-разрядная. Microsoft Windows Server 2012 Server Core/Datacenter/Essentials/Foundation/Standard 64-разрядная. Microsoft Windows Server 2012 R2 Server Core/Datacenter/Essentials/Foundation/Standard 64-разрядная. Windows Server 2016 Datacenter/Standard (вариант установки Server Core) (LTSB) 64-разрядная. Microsoft Windows Server 2019 Standard/Datacenter/Core 64-разрядная. Microsoft Windows Server 2019 RS5 Essentials/Standard 64-разрядная. Microsoft Windows Server 2022 Standard/Datacenter/Core 64-разрядная. Microsoft Windows Server 2025 Standard/Datacenter/Core 64-разрядная. Microsoft Windows Server 2022 21H2 Standard/Datacenter 64-разрядная. Microsoft Windows Small Business Server 2011 Standard 64-разрядная. Microsoft Windows Small Business Server 2011 Essentials 64-разрядная.

Операционные системы. Linux	Debian GNU/Linux 10.0, 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12 (Buster) 32-разрядная/64-разрядная. Debian GNU/Linux 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 11.8, 11.9, 11.10, 11.11 (Bullseye) 32-разрядная/64-разрядная. Debian GNU/Linux 12.0, 12.1, 12.2, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 12.13 (Bookworm) 32-разрядная/64-разрядная. Debian GNU/Linux 12.10, 12.11, 12.14 (Bookworm) ARM 64-разрядная. Debian GNU/Linux 13.0, 13.1, 13.2, 13.3 (Trixie) 64-разрядная. Ubuntu Server 10.04 LTS (Lucid Lynx) 32-разрядная/64-разрядная. Ubuntu Server 16.04 LTS (Xenial Xerus) 32-разрядная/64-разрядная. Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная. Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная. Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная. Ubuntu Server 22.04 LTS ARM 64-разрядная. Ubuntu Server 24.04 LTS (Noble Numbat) 64-разрядная. Ubuntu Server 26.04 LTS (Resolute Raccoon) 64-разрядная. Ubuntu Server 26.04 LTS ARM 64-разрядная. Ubuntu Desktop 10.04 LTS (Lucid Lynx) 32-разрядная/64-разрядная. Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32-разрядная/64-разрядная. CentOS 5.2 64-разрядная (поддерживается только Агентом администрирования для устаревших версий Linux). CentOS 5.4 64-разрядная (поддерживается только Агентом администрирования для устаревших версий Linux). CentOS 6.4 64-разрядная (поддерживается только Агентом администрирования для устаревших версий Linux). CentOS 6.6 32-разрядная/64-разрядная (поддерживается только Агентом администрирования для устаревших версий Linux). CentOS 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 64-разрядная. CentOS Stream 8 64-разрядная. CentOS Stream 9 64-разрядная. CentOS Stream 9 ARM 64-разрядная. CentOS Stream 10 64-разрядная. Red Hat Enterprise Linux Server 6.5, 6.6, 6.7, 6.8, 6.9, 6.10 32-разрядная/64-разрядная. Red Hat Enterprise Linux Server 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 64-разрядная. Red Hat Enterprise Linux Server 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 64-разрядная. Red Hat Enterprise Linux Server 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 64-разрядная. Red Hat Enterprise Linux Server 10.0, 10.1 64-разрядная. SUSE Linux Enterprise Server 12.5, 12.6, 12.7 64-разрядная. SUSE Linux Enterprise Server 15.0, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7 64-разрядная. SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7 ARM 64-разрядная. openSUSE Leap 15.0, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6 64-разрядная. EulerOS 2.0 SP10 64-разрядная. EulerOS 2.0 SP10 ARM 64-разрядная. Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.4) 32-разрядная. Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.4) 64-разрядная (поддерживается только Агентом администрирования для устаревших версий Linux). Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5) 64-разрядная. Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6) 64-разрядная. Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6) 64-разрядная. Astra Linux Special Edition РУСБ.10015-16 (исполнение 2) (очередное обновление 8.1) E2K. Astra Linux Special Edition РУСБ.10015-17 (очередное обновление 1.7.3) 64-разрядная. Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7) 64-разрядная. Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8) 64-разрядная. Astra Linux Special Edition РУСБ.10015-03 (очередное обновление 7.6) 64-разрядная. Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7) 64-разрядная. Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7) ARM 64-разрядная. Astra Linux Special Edition РУСБ.10265-01 (очередное обновление 8.1) E2K. Astra Linux Common Edition (очередное обновление 2.12) 64-разрядная. Альт Рабочая станция 11.2 ARM 64-разрядная.

Альт Рабочая станция 11 64-разрядная.

Альт Сервер 11.1 ARM 64-разрядная.

Альт Сервер 11 64-разрядная.

Альт Образование 11 64-разрядная.

Альт Рабочая станция 10.1 64-разрядная.

Альт Сервер 10.1 64-разрядная.

Альт Образование 10.1 64-разрядная.

Альт СП Сервер 10 32-разрядная/64-разрядная.

Альт СП Сервер 10 ARM 64-разрядная.

Альт СП Сервер 10 E2K.

Альт СП Рабочая станция 10 32-разрядная/64-разрядная.

Альт СП Рабочая станция 10 ARM 64-разрядная.

Альт СП Рабочая станция 10 E2K.

Альт 8 СП Сервер (ЛКНВ.11100-01) 32-разрядная/64-разрядная.

Альт 8 СП Сервер (ЛКНВ.11100-02) 32-разрядная/64-разрядная.

Альт 8 СП Сервер (ЛКНВ.11100-03) 32-разрядная/64-разрядная.

Альт 8 СП Сервер E2K.

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.

Альт 8 СП Рабочая станция E2K.

Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 64-разрядная.

Oracle Linux 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 64-разрядная.

Oracle Linux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7 64-разрядная.

Linux Mint 21.1, 21.2, 21.3 64-разрядная.

Linux Mint 22.0, 22.1, 22.2 64-разрядная.

AlterOS 7.5 64-разрядная.

AlterOS 2025 64-разрядная.

SberOS 3.4.0 64-разрядная.

SberOS 3.5.0 64-разрядная.

SberOS 3.6.1 64-разрядная.

Platform V SberLinux OS Server (SLO) 8.10.1 64-разрядная.

Platform V SberLinux OS Server (SLO) 9.1 64-разрядная.

Platform V SberLinux OS Server (SLO) 9.5.1 64-разрядная.

Platform V SberLinux OS Server (SLO) 9.6 64-разрядная.

Platform V SberLinux OS Server (SLO) 9.7 64-разрядная.

РЕД ОС 7.3 Сервер 64-разрядная.

РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.

РЕД ОС 8 64-разрядная.

РЕД ОС 8 ARM 64-разрядная.

ROSA Enterprise Linux Server 7.9 64-разрядная.

ROSA Enterprise Linux Desktop 7.9 64-разрядная.

РОСА "КОБАЛЬТ" 7.9 64-разрядная.

РОСА "ХРОМ" 12 64-разрядная.

AlmaLinux 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 64-разрядная.

AlmaLinux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 64-разрядная.

Rocky Linux 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 64-разрядная.

Rocky Linux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 64-разрядная.

Атлант, сборка Alcyone, версия 2022.02 64-разрядная.

МСВСфера 9.2 Сервер 64-разрядная.

МСВСфера 9.2 АРМ 64-разрядная.

МСВСфера 9.4 Сервер 64-разрядная.

МСВСфера 9.4 АРМ 64-разрядная.

МСВСфера 9.5 Сервер 64-разрядная.

МСВСфера 9.5 АРМ 64-разрядная.

СинтезМ Сервер 8.6 64-разрядная.

	СинтезМ Клиент 8.6 64-разрядная. ОСнова 2.9, 2.14 64-разрядная. ОСнова 3.0.5, 3.1 64-разрядная. Kylin 10 64-разрядная. EMIAS 1.0 64-разрядная. Amazon Linux 2 64-разрядная. Amazon Linux 2023 64-разрядная. МосОС Серверная 15.5 64-разрядная. МосОС Серверная 15.6 64-разрядная. ОС МЭШ 12 Для московских школ для компьютеров и ноутбуков (с телеметрией и поддержкой ДИТ) 64-разрядная. ОС МЭШ 12 Для московских школ для интерактивных панелей (с телеметрией и поддержкой ДИТ) 64-разрядная. M ОС (Moscow Electronic School) 12 Сервер 64-разрядная. МосТех 64-разрядная. МосТех Сервер 64-разрядная. Fedora Linux Server 41 64-разрядная. Fedora Linux Workstation 41 64-разрядная. Эльбрус 9.3.6 E2K
Операционные системы. macOS	Список поддерживаемых операционных систем см. в справке Kaspersky Endpoint Security для Mac.
Платформы виртуализации	Дополнительные сведения о поддерживаемых платформах виртуализации см. в справке Kaspersky Security для виртуальных сред Легкий агент.

В версиях Windows ниже версий Microsoft Windows Server 2008 R2 (для серверов) и Microsoft Windows 7 (для рабочих станций), Агент администрирования не поддерживает следующие функции:

- Передача обновлений (используется точками распространения).
- Прокси-сервер KSN (используется точками распространения).
- Задача поиска уязвимостей.

На устройствах под управлением Microsoft Windows 10 версии RS4 или RS5 Kaspersky Security Center может не обнаруживать некоторые уязвимости в папках, в которых включен учет регистра.

Перед установкой Агента администрирования на устройства под управлением Windows 7, Windows Server 2008 R2 или Windows MultiPoint Server 2011 убедитесь, что вы установили обновление безопасности KB3063858 для ОС Windows (Обновление безопасности для Windows 7 (KB3063858), Обновление безопасности для Windows 7 для систем на базе x64 (KB3063858), Обновление безопасности для Windows Server 2008 R2 x64 Edition (KB3063858).

В Microsoft Windows XP Агент администрирования может не выполнять некоторые операции правильно.

Вы можете установить или обновить Агент администрирования для Windows XP только в Microsoft Windows XP. Поддерживаемые редакции Microsoft Windows XP и соответствующие им версии Агента администрирования указаны в списке поддерживаемых операционных систем. Вы можете скачать необходимую версию Агента администрирования для Microsoft Windows XP с этой страницы.

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

Kaspersky Security Center Linux полностью поддерживает Агент администрирования той же версии или выше.

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

Совместимые приложения и решения "Лаборатории Касперского"

Kaspersky Security Center Linux поддерживает централизованное развертывание и управление всеми поддерживаемыми на данный момент приложениями и решениями "Лаборатории Касперского". Подробнее о версиях приложений и решений см. на странице "Жизненный цикл приложений".

Поддерживаемые приложения "Лаборатории Касперского":

- Kaspersky Endpoint Security для Windows (поддерживает файловые серверы)
- Kaspersky Endpoint Security для Linux (поддерживает файловые серверы)
- Kaspersky Endpoint Security для Linux Elbrus Edition
- Kaspersky Endpoint Security для Mac
- Kaspersky Endpoint Security для Android
- Kaspersky Endpoint Security для ОС Аврора
- Kaspersky Security для iOS
- Kaspersky Industrial CyberSecurity for Linux Nodes
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Endpoint Agent
- Kaspersky Embedded Systems Security для Windows
- Kaspersky Embedded Systems Security для Linux
- Kaspersky Security для виртуальных сред Легкий агент
- KATA Sandbox (один из компонентов Kaspersky Anti Targeted Attack Platform)
- Kaspersky Thin Client
- Kaspersky NGFW

- Kaspersky Sandbox
- Kaspersky Password Manager для бизнеса
- Kaspersky Vulnerability Management

Kaspersky Security Center Linux входит в состав следующих решений:

- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Managed Detection and Response
- Kaspersky Security для бизнеса Профессиональный

Подробнее о версиях приложений и решений см. на странице "Жизненный цикл приложений".

Известные проблемы и ограничения

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

О совместимости компонентов Kaspersky Security Center Linux

В таблице ниже вы найдете информацию о совместимости компонентов Kaspersky Security Center Linux.

Совместимость компонентов Kaspersky Security Center Linux

Компонент	Совместим с
Сервер администрирования Kaspersky Security Center 17 Linux	• Kaspersky Security Center Web Console следующих версий: 17, 16.3, 16.2. • Агент администрирования Kaspersky Security Center следующих версий: 17, 14*, 10.5**.
Kaspersky Security Center 17 Web Console	Сервер администрирования Kaspersky Security Center Linux следующих версий: 17, 16.3, 16.2.
Главный Сервер администрирования Kaspersky Security Center 17 Linux	Подчиненные Серверы администрирования: • Kaspersky Security Center Linux следующих версий: 17, 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1. • Kaspersky Security Center Windows следующих версий: 15.1.
Подчиненный Сервер администрирования Kaspersky Security Center 17 Linux	Главные Серверы администрирования: • Kaspersky Security Center Linux следующих версий: 17, 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1. • Kaspersky Security Center Windows следующих версий: 15.1.
Агент администрирования Kaspersky Security Center 17	Серверы администрирования: • Kaspersky Security Center Linux следующих версий: 17, 16.3, 16.2, 16.1, 16.0, 15.4, 15.3, 15.2, 15.1. • Kaspersky Security Center Windows следующих версий: 15.1.
Резервное копирование и восстановление данных Сервера администрирования Kaspersky Security Center	Резервное копирование и восстановление данных поддерживается в следующих версиях Сервера администрирования Kaspersky Security Center Linux: 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1.

*Эта версия поддерживает Microsoft Windows XP Professional Service Pack 3. Вы можете скачать эту версию Агента администрирования с этой страницы.

**Эта версия поддерживает Microsoft Windows XP Professional Service Pack 2. Вы можете запросить эту версию Агента администрирования в Службе технической поддержки.

Рекомендуется использовать последние версии Сервера администрирования Kaspersky Security Center и Kaspersky Security Center Web Console. В противном случае функциональность Kaspersky Security Center может быть ограничена. Вы можете установить и обновить Сервер администрирования Kaspersky Security Center и Kaspersky Security Center Web Console независимо друг от друга. В этом случае убедитесь, что версия установленного приложения Kaspersky Security Center Web Console совместима с версией Сервера администрирования, к которому вы подключаетесь:

Если у вас есть последняя версия Kaspersky Security Center Web Console и предыдущая версия Kaspersky Security Center и во время доменной аутентификации происходит ошибка, текст ошибки содержит стандартное сообщение.

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

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

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

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

Функция или свойство	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 17 Linux
Сервер администрирования		
Расположение системы управления базами данных (СУБД)	В локальной инфраструктуре	В локальной инфраструктуре (Microsoft SQL не поддерживается)
Операционная система для установки Сервера администрирования	Windows	Linux
Иерархия Серверов администрирования	✓	✓
Поддержка виртуальных Серверов администрирования	✓	✓
Развертывание отказоустойчивого кластера Kaspersky Security Center	✓ Только односайтовый отказоустойчивый кластер	✓ Начиная с версии Kaspersky Security Center 16.2 Linux поддерживается геораспределенный отказоустойчивый кластер.
Использование SNMP для отправки статистики Сервера администрирования приложениям сторонних производителей	✓	✓
Веб-сервер для публикации инсталляционных пакетов и других файлов	✓	✓

Функция или свойство	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 17 Linux
Консоль администрирования		
Тип Консоли администрирования	На базе MMC и веб-интерфейс	Веб-интерфейс
Операционная система для установки Консоли администрирования с веб-интерфейсом	Windows или Linux	Linux
Вход в консоль с использованием доменной аутентификации	✓	✓
Управление клиентскими устройствами и группами администрирования		
Максимальное количество управляемых устройств (на один Сервер администрирования)	100 000 (с Microsoft SQL Server)	50 000 (с PostgreSQL и Postgres Pro)
Опрос сети	✓	✓
Защита устройств под управлением Windows, macOS и Linux	✓	✓
Защита мобильных устройств	✓ Базовое управление мобильными устройствами	✓ MDM и использование функциональности Kaspersky Secure Mobility Management (по лицензии).
Управление защитой виртуальных машин	✓	✓
Защита публичной облачной инфраструктуры	✓	—
Удаленное подключение к рабочему столу клиентского устройства	✓	✓
Шифрование и защита данных	✓ На управляемых устройствах с операционной системой Windows с установленным Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Mac.	✓ На управляемых устройствах с операционной системой Windows с установленным Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Mac.
Поддержка кластеров и массивов серверов в группах администрирования	✓	✓
Иерархия групп администрирования	✓	✓
Добавление шлюза соединения в демилитаризованной зоне в качестве точки распространения	✓ (не поддерживается для Web Console)	✓
Работа с пользователями		
Создание учетных записей пользователей, контроль учетных записей	✓	✓
Управление приложениями "Лаборатории Касперского"		
Политики приложений	✓	✓
Задачи для приложений "Лаборатории Касперского"	✓	✓
Kaspersky Security Network	✓	✓
Прокси-сервер KSN	✓	✓
Kaspersky Private Security Network	✓	✓
Централизованное распространение лицензионных ключей приложений "Лаборатории Касперского"	✓	✓
Удаленная диагностика клиентских устройств	✓	✓

Функция или свойство	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 17 Linux
Автоматическое обновление приложений "Лаборатории Касперского"	✓	✓
Поддержка Адаптивного контроля аномалий	✓	✓
Управление безопасностью устройств	✓	✓
Управление безопасностью, ориентированной на пользователя	✓	✓
Управление системами		
Развертывание операционных систем на клиентских устройствах	✓	—
Управление сторонними лицензиями	✓	Будет реализовано в 2026 году
Использовать Сервер администрирования в роли WSUS-сервера	✓	✓ (только в пассивном режиме поиска Центра обновления Windows)
Управление приложениями сторонних производителей на клиентских устройствах		
Установка обновлений приложений сторонних производителей и поиск уязвимостей в приложениях сторонних производителей	✓	✓
Импорт и экспорт категорий приложений	✓ (не поддерживается для Web Console)	Будет реализовано в 2026 году
Мониторинг, отчеты и аудит		
Работа с ревизиями объектов	✓	✓
Сравнение ревизий политики	✓	✓
Просмотр и работа с алертами, обнаруженными Kaspersky Endpoint Detection and Response Optimum	✓	✓
Уведомления о событиях, произошедших на управляемых устройствах	✓	✓
Мониторинг состояния политик и задач	✓	✓
Экспорт всех событий из списка событий на устройстве	✓ (не поддерживается для Web Console)	✓
Интеграции		
Интеграция с Kaspersky Managed Detection and Response	✓	✓
Интеграция с SIEM-системами	✓	✓
Агрегирование алертов и выполнение действий по реагированию с помощью Active Directory, KASAP и Kaspersky TIP Sandbox	—	✓ Вам нужно активировать Сервер администрирования по лицензии Kaspersky Security для бизнеса Профессиональный, а затем распространить лицензионный ключ Kaspersky Security для бизнеса Профессиональный на управляемые приложения.

О Kaspersky Security Center Cloud Console

Если вы используете Kaspersky Security Center как приложение, работающее локально, то это означает, что вы устанавливаете Kaspersky Security Center, включая Сервер администрирования, на локальное устройство и управляете системой безопасности сети с помощью Консоли администрирования на основе консоли управления Microsoft Management Console (MMC) (доступно только для Kaspersky Security Center Windows) или с помощью Kaspersky Security Center Web Console.

Вместо этого вы можете использовать Kaspersky Security Center как облачную службу. В этом случае Kaspersky Security Center устанавливается за вас экспертами "Лаборатории Касперского" в облачном окружении и "Лаборатория Касперского" предоставляет вам доступ к Серверу администрирования в качестве службы. Вы управляете системой безопасности сети с помощью Консоли администрирования на основе облачной службы, которая называется Kaspersky Security Center Cloud Console. Эта консоль имеет интерфейс, аналогичный интерфейсу приложения Kaspersky Security Center Web Console.

Интерфейс и документация Kaspersky Security Center Cloud Console доступны на следующих языках:

- английском;
- французском;
- немецком;
- итальянском;
- японском;
- португальском (Бразилия);
- русском;
- упрощенном китайском;
- испанском;
- испанском (Латинская Америка);
- традиционном китайском.

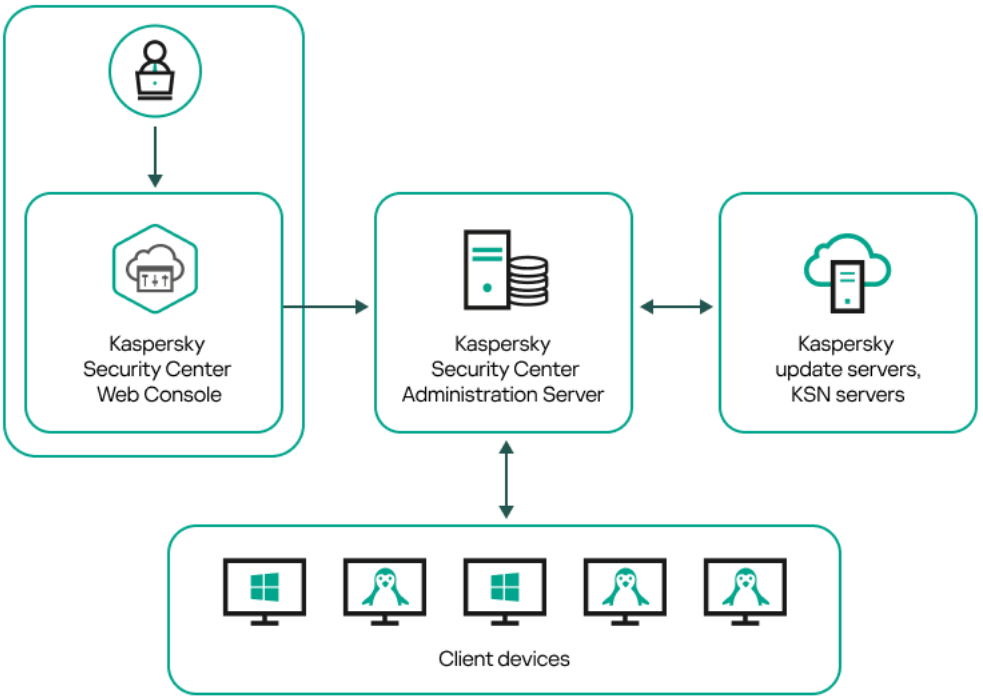
Больше информации о Kaspersky Security Center Cloud Console и функциональности доступно в документации Kaspersky Security Center Cloud Console и в документации Kaspersky Endpoint Security для бизнеса.

Архитектура и основные понятия

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

Архитектура приложения

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



Архитектура приложения Kaspersky Security Center Linux

Приложение Kaspersky Security Center Linux включает в себя следующие основные компоненты:

- **Kaspersky Security Center Web Console**. Представляет собой веб-интерфейс для создания и управления системой защиты сети организации-клиента, находящейся под управлением Kaspersky Security Center.
- **Сервер администрирования Kaspersky Security Center** (далее также *Сервер*). Осуществляет функции централизованного хранения информации об установленных в сети организации приложениях и управления ими.
- **Серверы обновлений "Лаборатории Касперского"**. HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложений.

- **Серверы KSN**. Серверы содержат оперативную базу знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

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

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

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

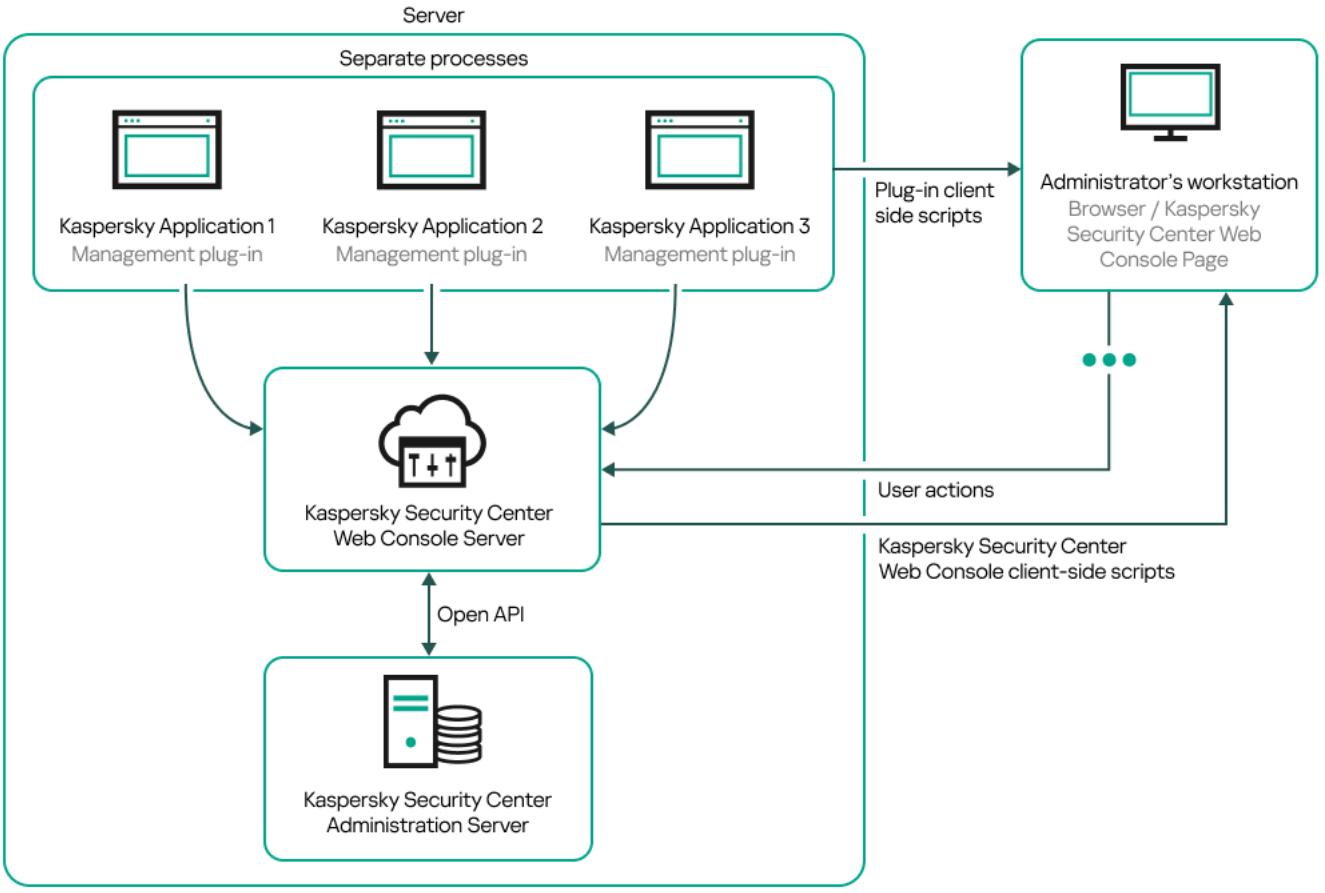


Схема развертывания Сервера администрирования Kaspersky Security Center Linux и Kaspersky Security Center Web Console

Развертывание плагинов управления приложениями "Лаборатории Касперского", установленных на защищаемых устройствах (отдельный плагин для каждого приложения), происходит одновременно с развертыванием Сервера Kaspersky Security Center Web Console.

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

Когда вы выполняете определенные действия в Kaspersky Security Center Web Console, Сервер Kaspersky Security Center Web Console взаимодействует с Сервером администрирования Kaspersky Security Center Linux по OpenAPI. Сервер Kaspersky Security Center Web Console запрашивает необходимые данные у Сервера администрирования Kaspersky Security Center Linux и отображает результаты ваших действий в Kaspersky Security Center 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; используется также на подчиненных серверах для приема подключений от главного Сервера (например, если подчиненный Сервер находится в демилитаризованной зоне)	Управление клиентскими устройствами и подчиненными Серверами администрирования. Вы можете изменить номер порта по умолчанию для приема подключений от Агентов администрирования при настройке портов подключения во время установки Kaspersky Security Center 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)	Использование утилиты klakaut для автоматизации работы Kaspersky Security Center Linux	Работа с утилитой klakaut. Утилита klakaut и справочная система для нее расположены в папке установки Kaspersky Security Center Linux. По умолчанию порт закрыт. Если вы хотите использовать утилиту klakaut для автоматизации работы Kaspersky Security Center Linux, откройте порт 13291 с помощью утилиты klscflag.

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
13299	klserver	TCP (TLS)	Прием подключений от Identity and Access Manager (IAM) к Серверу администрирования; прием подключений к Серверу администрирования через OpenAPI	Управление Сервером администрирования с помощью Kaspersky Security Center Web Console; работа с 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 необязательный и закрыт по умолчанию. В целях безопасности рекомендуется использовать TCP-порт 13000.
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.
17111 (только если на устройстве запущена служба прокси-сервера KSN)	ksnproxy	HTTPS	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 приложений от управляемых устройств	Прокси-сервер активации для управляемых устройств. Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования (в подразделе **Дополнительные порты** раздела **Общий**).
13292 (только если вы управляете мобильными устройствами)	klserver	TCP (TLS)	Прием подключений от мобильных устройств	Управление мобильными устройствами. Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования в Консоли администрирования или в Kaspersky Security Center Web Console.
19170	klserver	HTTPS (TLS)	Туннелирование соединения с управляемыми устройствами с помощью утилиты klsctunnel	Удаленное подключение к управляемым устройствам с помощью Kaspersky Security Center Web Console. Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования (**Общие → Порты подключения → Туннельное RDP-подключение**).
4444	kliam	HTTPS	Аутентификация с использованием протокола OpenID Connect	Обмен токенами аутентификации между браузером и Identity and Access Manager (IAM).
9050	kliam	HTTPS	Подключение к Серверу администрирования с помощью IAM	Обмен токенами аутентификации между Kaspersky Security Center Web Console и IAM.

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

В таблице ниже указан порт, который используется Сервером iOS™ MDM (только если вы управляете мобильными устройствами).

Порт, используемый Сервером iOS MDM

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

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

Порт, используемый Сервером Kaspersky Security Center Web Console

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
8080	Node.js: серверный JavaScript	TCP (TLS)	Прием подключений от браузера и передача в Kaspersky Security Center Web Console	Kaspersky Security Center Web Console. Вы можете изменить номер порта, указанного по умолчанию, во время установки Kaspersky Security Center Web Console. Если вы устанавливаете Kaspersky Security Center Web Console на устройство с операционной системой Альт Linux, то необходимо указать номер порта, отличный от 8080, так как порт 8080 используется операционной системой.

В таблице ниже указаны порты, которые используются 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	Перенос обновлений приложений из Агента администрирования в локально установленные приложения "Лаборатории Касперского" с помощью компонента FileTransferBridge.	Управляемые устройства, которые получают обновления приложения "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-сервера KSN)	ksnproxy	UDP	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN. Вы можете изменить значения портов по умолчанию в свойствах точки распространения.
17111 (только если на устройстве запущена служба прокси-сервера KSN)	ksnproxy	HTTPS	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN. Вы можете изменить значения портов по умолчанию в свойствах точки распространения.
13295 (только если вы используете точку распространения в качестве push-сервера)	klnagent	TCP (TLS)	Прием подключений от клиентских устройств	Push-сервер. Вы можете изменить значения портов по умолчанию в свойствах точки распространения.
8060	klcsweb	TCP	Передача на клиентские устройства опубликованных инсталляционных пакетов	Публикация инсталляционных пакетов. Вы можете изменить значения портов, заданных по умолчанию, в разделе **Веб-сервер** окна свойств Сервера администрирования.
8061	klcsweb	TCP (TLS)	Передача на клиентские устройства опубликованных инсталляционных пакетов	Публикация инсталляционных пакетов. Вы можете изменить значения портов, заданных по умолчанию, в разделе **Веб-сервер** окна свойств Сервера администрирования.

В таблице ниже показаны порты, используемые на устройстве контроллера домена.

Порты, используемые на устройстве контроллера домена

Номер порта	Протокол	Назначение порта	Область
389	LDAP по протоколу TCP или UDP	Подключение к LDAP-серверу	Опрос контроллеров домена
636	LDAP по протоколу TLS	Подключение к LDAP-серверу	Опрос контроллеров домена

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

Порт, используемый на нераспределенном клиентском устройстве

Номер порта	Протокол	Назначение порта	Область
22	SSH	Подключение к клиентскому устройству по протоколу SSH	Удаленная установка приложений "Лаборатории Касперского".

Порты, используемые приложением Kaspersky Security Center Web Console

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

Порты, используемые приложением Kaspersky Security Center 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 получения 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 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 приложения Kaspersky Security Center Web Console.
4222	Kaspersky Security Center Web Console NATS	HTTPS	API-порты Message Broker на основе NATS, которые используются для связи между Kaspersky Security Center Web Console и плагинами управления. Порт 8222 используется для мониторинга NATS.	Взаимодействие между Kaspersky Security Center Web Console и плагинов управления
4444	Identity and Access Manager (IAM)	HTTPS	Порт, который используется протоколом аутентификации OpenID Connect.	Обмен токенами аутентификации между Kaspersky Security Center Web Console и Identity and Access Manager (IAM)
9050	IAM	HTTPS	Порт, который используется IAM.	Взаимодействие между Kaspersky Security Center Web Console и IAM

Основные понятия

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

Сервер администрирования

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

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

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

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

Полный список параметров установки см. в статье Установка Kaspersky Security Center Linux.

Сервер администрирования выполняет следующие функции:

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

Правило именования Серверов администрирования в интерфейсе приложения

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

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

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

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

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

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

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

Виртуальный Сервер администрирования

Виртуальный Сервер администрирования (далее также *виртуальный Сервер*) – компонент приложения Kaspersky Security Center Linux, 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 приложения "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://<Web Server name>:<HTTPS port>/public/<object>`

где:

- `<Web Server name>` – имя Веб-сервера Kaspersky Security Center.
- `<HTTPS port>` – HTTPS-порт Веб-сервера, заданный администратором. HTTPS-порт можно задать в разделе **Веб-сервер** окна свойств Сервера администрирования. По умолчанию установлен порт 8061.
- `<object>` – 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.

Веб-сервер Kaspersky Security Center Linux

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

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

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

Настройка Веб-сервера

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

Параметры Веб-сервера на шлюзе соединения

Реализована отдельная служба Веб-сервера на точке распространения в режиме шлюза соединения, что позволяет работать с мобильными устройствами, подключенными к Kaspersky Security Center Linux. Эта служба отвечает за передачу инсталляционных пакетов приложений и управляющих профилей на устройства без прямого подключения к Серверу администрирования. Файлы передаются по мере обработки службой запросов на файлы HTTP/HTTPS на шлюзе соединения.

Служба Веб-сервера на шлюзе соединения устанавливается вместе с Агентом администрирования Linux. Чтобы использовать эту функцию, вам нужно назначить устройство, которое будет выполнять роль точки распространения в режиме шлюза соединения, для использования в качестве Веб-сервера, а затем указать соответствующие параметры. Подробнее о настройке параметров Веб-сервера на шлюзе соединения см. в справке Kaspersky Secure Mobility Management.

Агент администрирования

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

Устройство, на которое установлен Агент администрирования, называется *управляемым устройством* или *устройством*. Инсталляционный пакет Агента администрирования можно загрузить из следующих источников:

- из хранилища Сервера администрирования (необходимо, чтобы был установлен Сервер администрирования);
- сайт "Лаборатории Касперского".

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

- под именем "Kaspersky Network Agent";
- с автоматическим типом запуска при старте операционной системы;
- с помощью корневой учетной записи.

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

- с именем "Kaspersky Security Center Network Agent";
- с автоматическим типом запуска при старте операционной системы;
- с использованием учетной записи LocalSystem.

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

- с именем "com.kaspersky.klnagent.core";
- с автоматическим типом запуска при старте операционной системы;
- с использованием корневой учетной записи.

Названия служебных процессов:

- Для Linux:
  - klnagent64.service (для 64-разрядной операционной системы)
  - klnagent.service (для 32-разрядной операционной системы)
- Для Windows:
  - klnagent
- Для macOS:
  - com.kaspersky.klnagent

По умолчанию Агент администрирования устанавливается в следующих директориях:

- Для Linux:
  - для 32-разрядной системы: /opt/kaspersky/klnagent/
  - для 64-разрядной системы: /opt/kaspersky/klnagent64/
- Для Windows:
  - для 32-разрядной системы: C:\Program Files\Kaspersky Lab\NetworkAgent
  - для 64-разрядной системы: C:\Program Files (x86)\Kaspersky Lab\NetworkAgent
- Для macOS:
  - для 64-разрядной системы: /Library/Application Support/Kaspersky Lab/klnagent/Binaries/klnagent

Для устройств с операционной системой Windows вы можете указать папку для установки Агента администрирования в параметрах инсталляционного пакета. Для устройств с операционной системой Linux Агент администрирования может быть установлен только в директорию по умолчанию.

Папка установки Агента администрирования также содержит утилиты для управления и диагностики работы Агента администрирования, например утилиты klmover и klnagchk.

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.

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 клиентских устройств, объединенных по какому-либо признаку с целью управления устройствами группы как единым целым в Kaspersky Security Center Linux.

Для всех управляемых устройств в группе администрирования устанавливаются:

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

Управляемое устройство может входить в состав только одной группы администрирования.

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

Управляемое устройство

Управляемое устройство – это устройство с операционной системой Linux, Windows или macOS, на котором установлен Агент администрирования. Вы можете управлять такими устройствами с помощью задач и политик для приложений, установленных на устройствах. Вы также можете формировать отчеты для управляемых устройств.

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

Устройство может находиться под управлением только одного Сервера администрирования. Количество устройств, которые могут управляться одним Сервером администрирования, зависит от конфигурации устройства, на котором размещен Сервер администрирования и от ограничений СУБД.

Нераспределенное устройство

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

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

Рабочее место администратора

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

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

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

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

Веб-плагин управления

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

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

Плагин управления предоставляет следующие возможности:

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

Политики

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

Статус политики

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

Политики действуют по следующим правилам:

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

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

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

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

Профили политик работают по следующим правилам:

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

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 Linux 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 Linux управляет работой приложений безопасности "Лаборатории Касперского", установленных на устройствах, путем создания и запуска *задач*. С помощью задач выполняются установка, запуск и остановка приложений, проверка файлов, обновление баз и модулей приложений, другие действия с приложениями.

Вы можете создать задачу для приложения, только если для этого приложения установлен плагин управления.

Задачи могут выполняться на Сервере администрирования и на устройствах.

Задачи, которые выполняются на Сервере администрирования:

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

На устройствах выполняются следующие типы задач:

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

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

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

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

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

Для каждого приложения вы можете создавать любое количество групповых задач, глобальных задач и локальных задач.

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

Запуск задач на устройстве выполняется только в том случае, если запущено приложение, для которого созданы эти задачи.

Результаты выполнения задач сохраняются в системном журнале событий и журнале событий Kaspersky Security Center Linux 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 применения 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. Также можно выбрать устройства, обнаруженные в сети Сервером администрирования.

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

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

- Указать выборку устройств.

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

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

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

Взаимосвязь политики и локальных параметров приложения

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

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

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

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

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

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

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

Точка распространения

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

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

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

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

  Можно включить прокси-сервер KSN на стороне точки распространения, чтобы устройство исполняло роль прокси-сервера KSN. В этом случае на устройстве запустится служба прокси-сервера KSN.

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

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

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

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

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

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

Kaspersky Security Center 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 приложения, изменены не будут.

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

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

Для работы точки распространения требуется не менее 4 ГБ свободного места на диске. Если объем свободного места на диске точки распространения меньше 2 ГБ, Kaspersky Security Center Linux создает проблему безопасности с уровнем важности *Предупреждение*. Проблема безопасности будет опубликована в свойствах устройства в разделе **Проблемы безопасности**.

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

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

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

Шлюз соединения

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

Шлюз соединения может принимать соединения от 10 000 устройств.

Существует два варианта использования шлюзов соединения:

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

  Шлюз соединения не изменяет и не обрабатывает данные, передаваемые от Агентов администрирования на Сервер администрирования. Шлюз соединения не записывает эти данные в буфер и, следовательно, не может принимать данные от Агента администрирования и затем передавать их на Сервер администрирования. Если Агент администрирования пытается подключиться к Серверу администрирования через шлюз соединения, но шлюз соединения не может подключиться к Серверу администрирования, Агент администрирования воспринимает это как недоступный Сервер администрирования. Все данные остаются на Агенте администрирования (не на шлюзе соединения).

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

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

- Вы также можете использовать шлюзы соединения в сети. Например, автоматически назначаемые точки распространения также становятся шлюзами соединения 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.

Виртуальные Серверы администрирования

В рамках физического Сервера администрирования можно создать несколько виртуальных Серверов администрирования, во многом подобных подчиненным Серверам. По сравнению с моделью разделения доступа, основанной на списках контроля доступа (ACL), модель виртуальных Серверов более функциональна и предоставляет большую степень изоляции. В дополнение к структуре групп администрирования, предназначенной для назначения устройствам политик и задач, каждый виртуальный Сервер администрирования имеет собственную группу нераспределенных устройств, собственные наборы отчетов, выборки устройств и события, инсталляционные пакеты, правила перемещения и т. д. Функциональность виртуальных Серверов администрирования может быть использована как поставщиками услуг (xSP) для максимальной изоляции разных заказчиков друг от друга, так и крупными организациями со сложной структурой и большим количеством администраторов.

Виртуальные Серверы во многом подобны подчиненным Серверам администрирования, однако имеют следующие отличия:

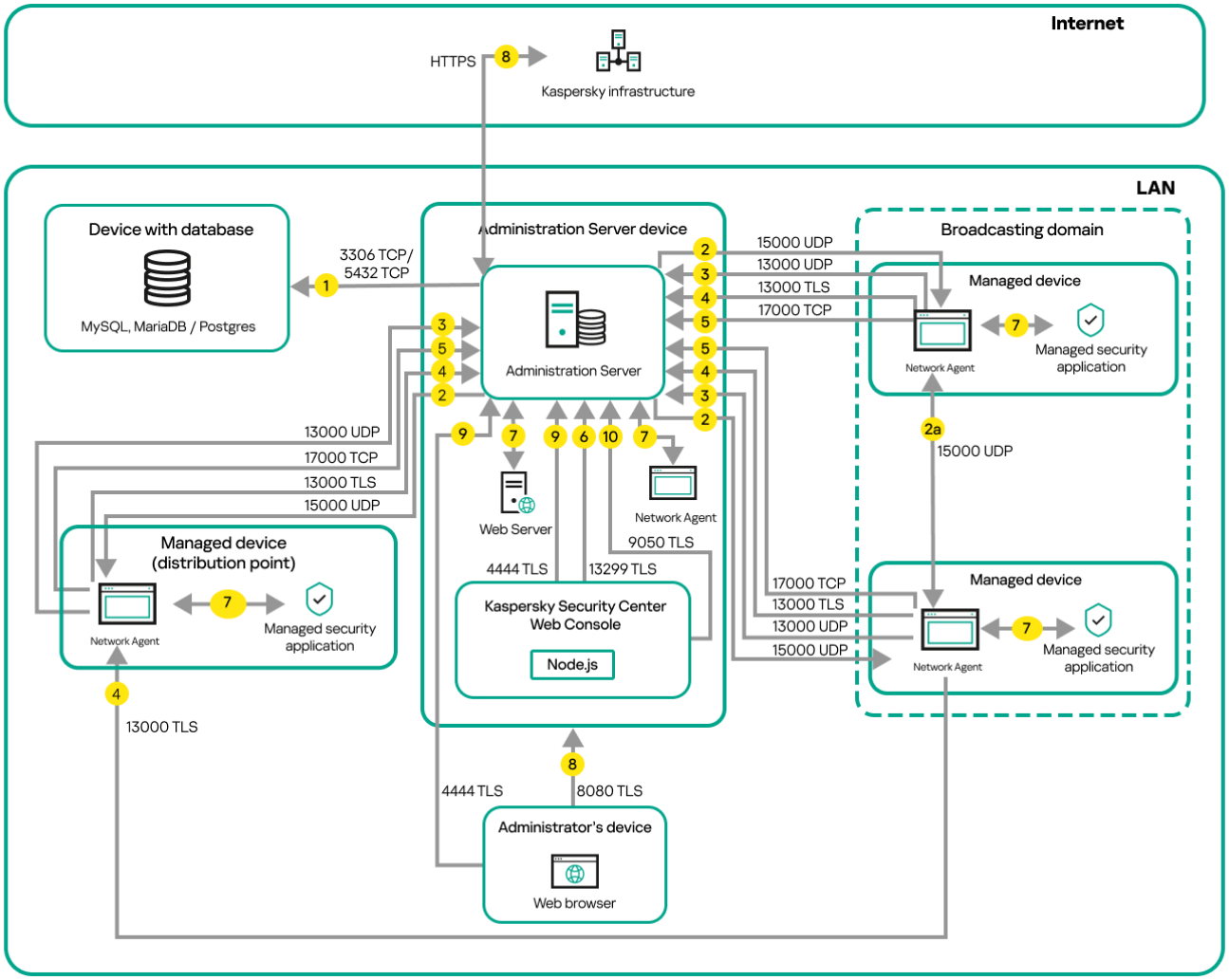
- виртуальный Сервер не имеет большинства глобальных параметров и собственных TCP-портов;
- у виртуального Сервера не может быть подчиненных Серверов;
- у виртуального Сервера не может быть собственных виртуальных Серверов;
- на физическом Сервере администрирования видны устройства, группы, события и объекты с управляемых устройств (элементы карантина, реестра приложений и прочее) всех его виртуальных Серверов;
- виртуальный Сервер может сканировать сеть только посредством подключенных к нему точек распространения.

Схемы трафика данных и использования портов

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

Сервер администрирования и управляемые устройства в локальной сети (LAN)

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



Сервер администрирования и управляемые устройства в локальной сети (LAN)

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

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

1. Сервер администрирования передает данные в базу данных. Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server и MariaDB Server, или порт 5432 для PostgreSQL Server или Postgres Pro Server). Подробную информацию см. в документации СУБД.

2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000.

   Агенты администрирования отправляют запросы друг другу в пределах одного широковещательного домена. Затем данные отправляются на Сервер администрирования и используются для определения пределов широковещательного домена и для автоматического назначения точек распространения (если этот параметр включен).

   Если Сервер администрирования не имеет прямого доступа к управляемым устройствам, запросы на связь с Сервером администрирования на эти устройства не отправляются напрямую.

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

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

4. Сервер администрирования принимает подключения от Агентов администрирования и от подчиненных Серверов администрирования через TLS-порт 13000.

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

5. Управляемые устройства (кроме мобильных устройств) запрашивают активацию через TCP-порт 17000. В этом нет необходимости, если устройство имеет собственный доступ в интернет; в этом случае устройство отправляет данные на серверы "Лаборатории Касперского" напрямую через интернет.

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

   Компонент Identity and Access Manager (IAM) подключается к Серверу администрирования по TLS-порту 13299.

7. Приложения на одном устройстве обмениваются локальным трафиком (либо на Сервере администрирования, либо на управляемом устройстве). Открывать внешние порты не требуется.

8. Данные от Сервера администрирования к серверам "Лаборатории Касперского" (например, данные KSN, информация о лицензиях) и данные от серверов "Лаборатории Касперского" к Серверу администрирования (например, обновления приложений и обновления антивирусных баз) передаются по протоколу HTTPS.

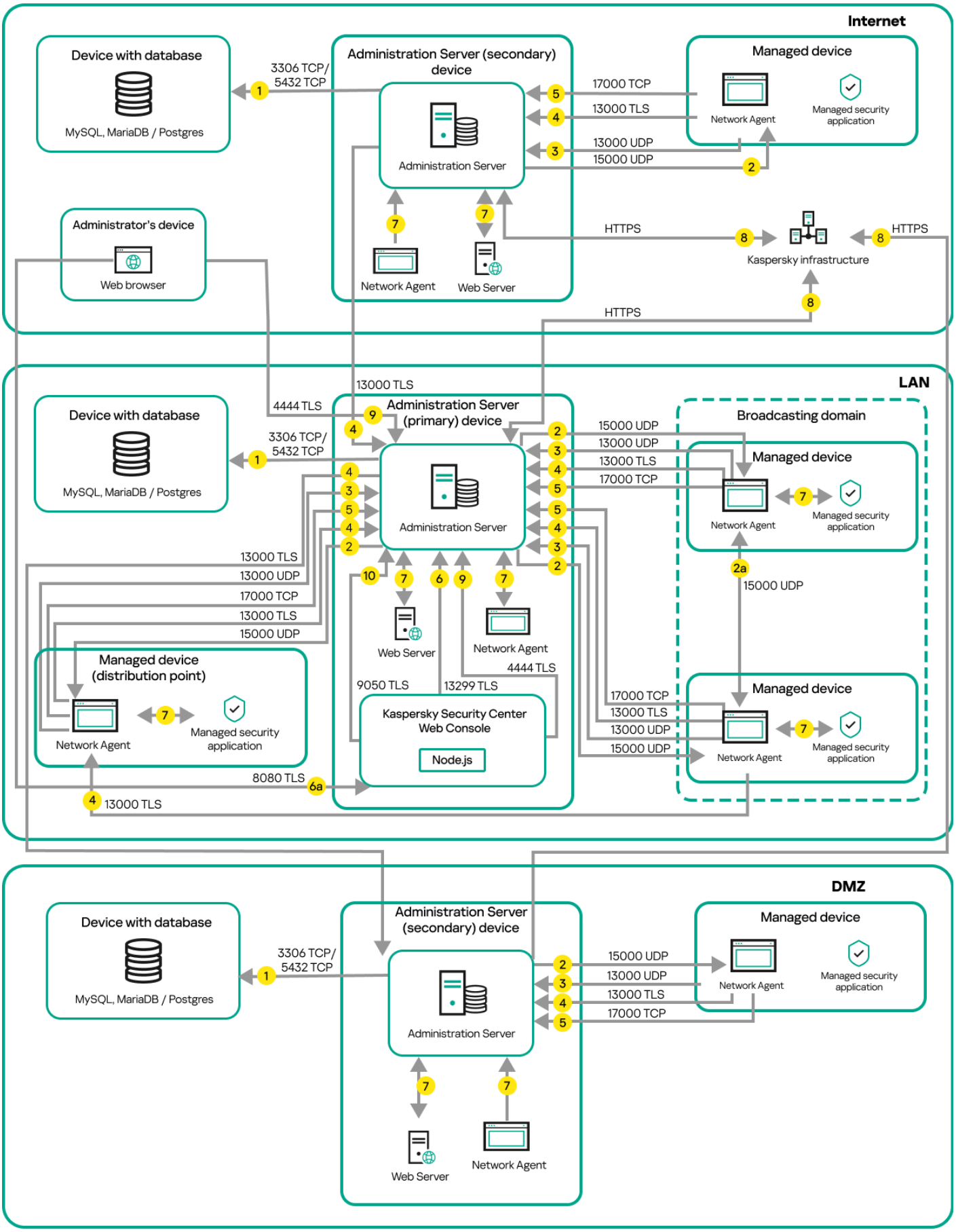
   Если вы не хотите иметь доступ в интернет на вашем Сервере администрирования, вам нужно управлять этими данными вручную.

9. Сервер Kaspersky Security Center Web Console и браузер (используемый с Kaspersky Security Center Web Console) подключаются к Серверу администрирования по протоколу аутентификации OpenID Connect по TLS-порту 4444.

10. Сервер Kaspersky Security Center Web Console подключается к Серверу администрирования по TLS-порту 9050.

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

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



Иерархия Серверов администрирования: главный Сервер администрирования и два подчиненных Сервера администрирования

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

1. Сервер администрирования передает данные в базу данных. Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server и MariaDB Server или порт 5432 для PostgreSQL Server или Postgres Pro Server). Подробную информацию см. в документации СУБД.

2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000.

   Агенты администрирования отправляют запросы друг другу в пределах одного широковещательного домена. Затем данные отправляются на Сервер администрирования и используются для определения пределов широковещательного домена и для автоматического назначения точек распространения (если этот параметр включен).

   Если Сервер администрирования не имеет прямого доступа к управляемым устройствам, запросы на связь с Сервером администрирования на эти устройства не отправляются напрямую.

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

4. Сервер администрирования принимает подключения от Агентов администрирования и от подчиненных Серверов администрирования через TLS-порт 13000.

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

5. Управляемые устройства (кроме мобильных устройств) запрашивают активацию через TCP-порт 17000. В этом нет необходимости, если устройство имеет собственный доступ в интернет; в этом случае устройство отправляет данные на серверы "Лаборатории Касперского" напрямую через интернет.

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

   Компонент Identity and Access Manager (IAM) подключается к Серверу администрирования по TLS-порту 13299.

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

7. Приложения на одном устройстве обмениваются локальным трафиком (либо на Сервере администрирования, либо на управляемом устройстве). Открывать внешние порты не требуется.

8. Данные от Сервера администрирования к серверам "Лаборатории Касперского" (например, данные KSN, информация о лицензиях) и данные от серверов "Лаборатории Касперского" к Серверу администрирования (например, обновления приложений и обновления антивирусных баз) передаются по протоколу HTTPS.

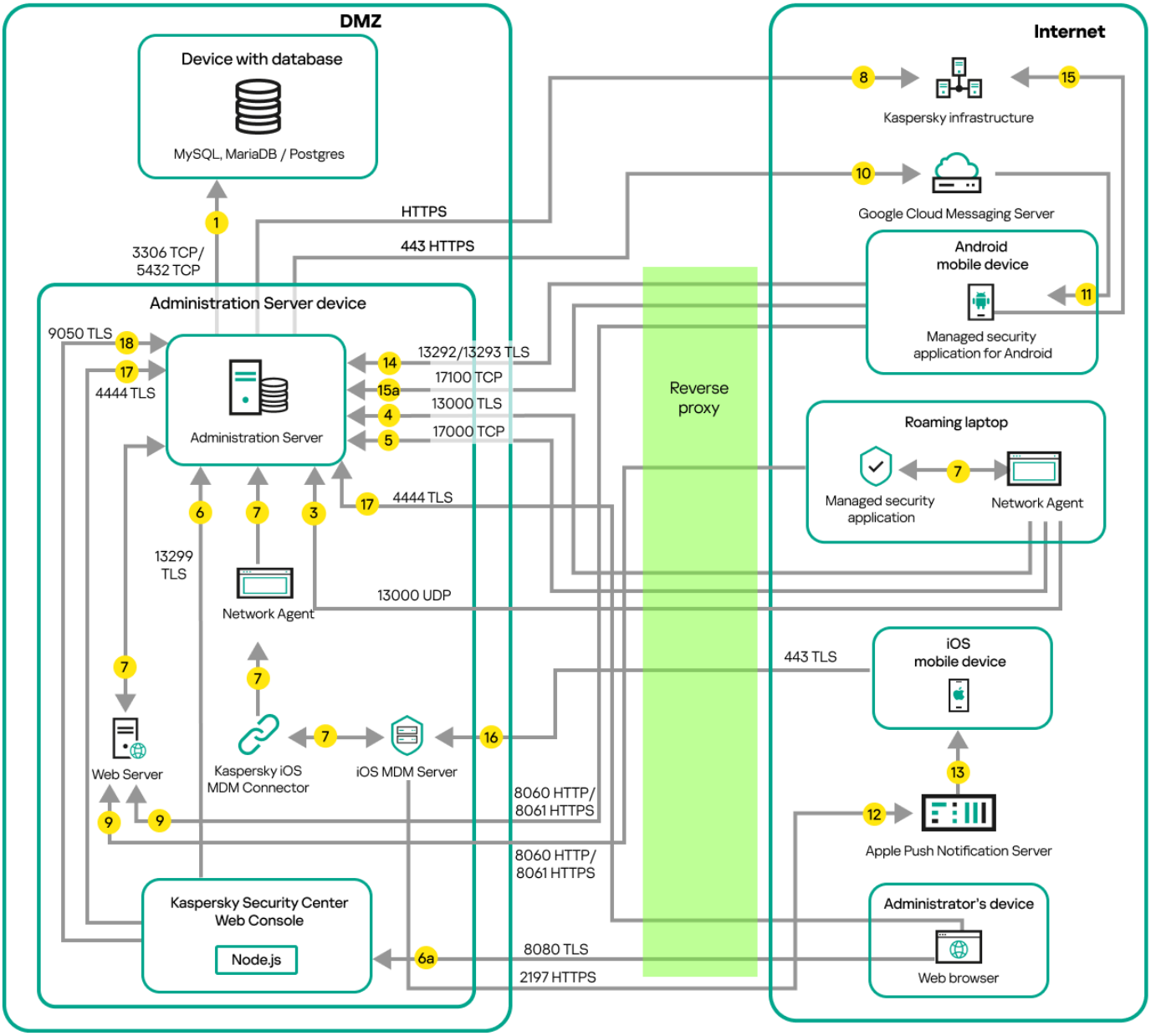
   Если вы не хотите иметь доступ в интернет на вашем Сервере администрирования, вам нужно управлять этими данными вручную.

9. Сервер Kaspersky Security Center Web Console и браузер (используемый с Kaspersky Security Center Web Console) подключаются к Серверу администрирования по протоколу аутентификации OpenID Connect по TLS-порту 4444.

10. Сервер Kaspersky Security Center Web Console подключается к Серверу администрирования по TLS-порту 9050.

Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете; использование обратного прокси-сервера

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



Сервер администрирования в локальной сети; управляемые устройства подключаются к Серверу администрирования с помощью обратного прокси-сервера

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

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

1. Сервер администрирования передает данные в базу данных. Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server и MariaDB Server или порт 5432 для PostgreSQL Server или Postgres Pro Server). Подробную информацию см. в документации СУБД.

2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000.

   Агенты администрирования отправляют запросы друг другу в пределах одного широковещательного домена. Затем данные отправляются на Сервер администрирования и используются для определения пределов широковещательного домена и для автоматического назначения точек распространения (если этот параметр включен).

   Если Сервер администрирования не имеет прямого доступа к управляемым устройствам, запросы на связь с Сервером администрирования на эти устройства не отправляются напрямую.

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

4. Сервер администрирования принимает подключения от Агентов администрирования и от подчиненных Серверов администрирования через TLS-порт 13000.

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

5. Управляемые устройства (кроме мобильных устройств) запрашивают активацию через TCP-порт 17000. В этом нет необходимости, если устройство имеет собственный доступ в интернет; в этом случае устройство отправляет данные на серверы "Лаборатории Касперского" напрямую через интернет.

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

   Компонент Identity and Access Manager (IAM) подключается к Серверу администрирования по TLS-порту 13299.

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

7. Приложения на одном устройстве обмениваются локальным трафиком (либо на Сервере администрирования, либо на управляемом устройстве). Открывать внешние порты не требуется.

8. Данные от Сервера администрирования к серверам "Лаборатории Касперского" (например, данные KSN, информация о лицензиях) и данные от серверов "Лаборатории Касперского" к Серверу администрирования (например, обновления приложений и обновления антивирусных баз) передаются по протоколу HTTPS.

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

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

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

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

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

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

14. Только для мобильных устройств: управляемое приложение передает данные на Сервер администрирования (или на шлюз соединений) через TLS-порт 13292/13293 напрямую или через обратный прокси-сервер.

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

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

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

17. Сервер Kaspersky Security Center Web Console и браузер (используемый с Kaspersky Security Center Web Console) подключаются к Серверу администрирования по протоколу аутентификации OpenID Connect по TLS-порту 4444.

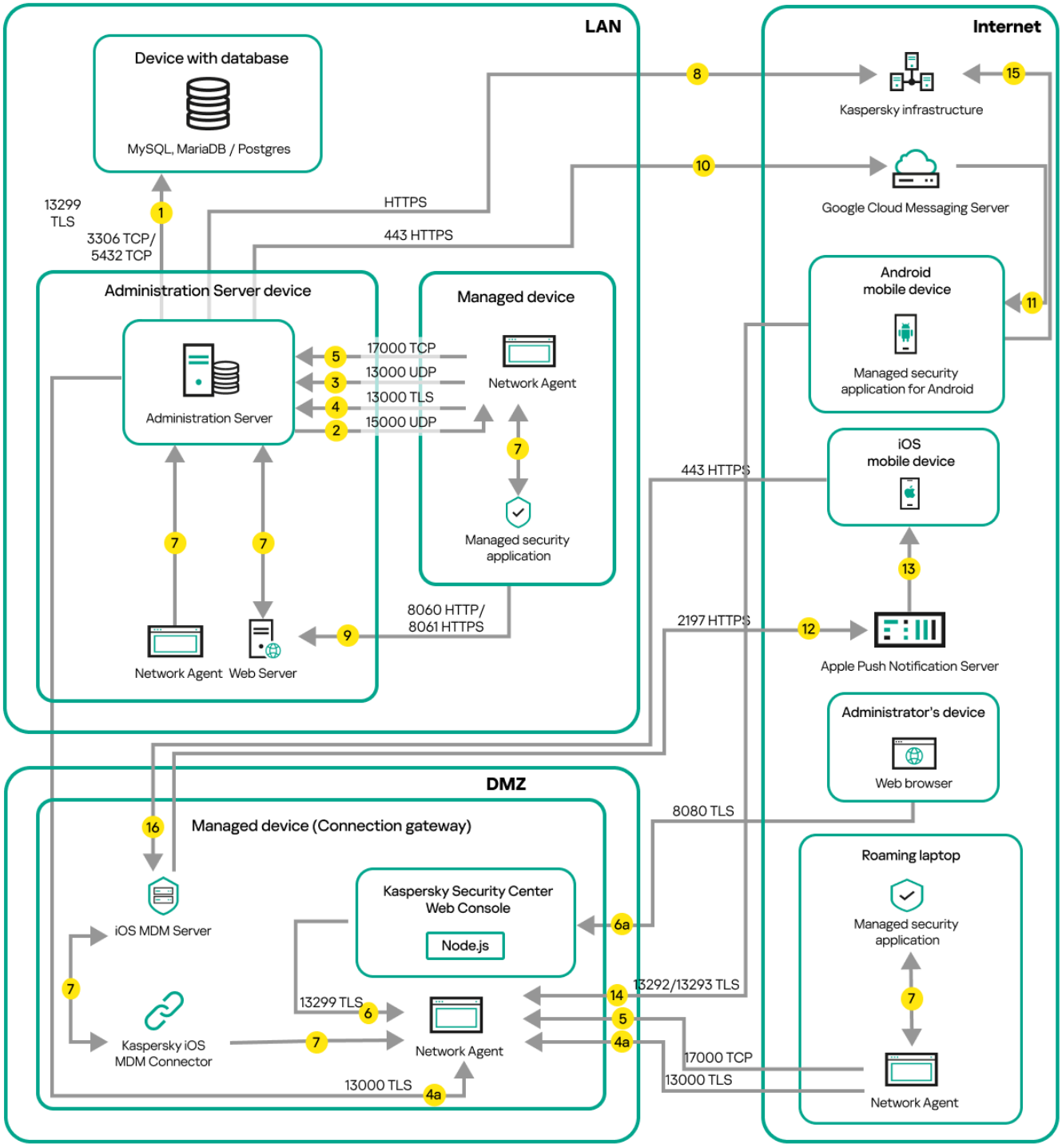
18. Сервер Kaspersky Security Center Web Console подключается к Серверу администрирования по TLS-порту 9050.

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

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

Эта схема развертывания рекомендуется, если вы не хотите, чтобы управляемые устройства подключались непосредственно к Серверу администрирования, и не хотите использовать обратный прокси-сервер или корпоративный сетевой экран.

Для этой схемы развертывания не поддерживается доменная аутентификация (единый вход), предоставляемая Identity and Access Manager (IAM).



Управляемые мобильные устройства, подключенные к Серверу администрирования через шлюз соединения

На этом рисунке управляемые устройства подключены к Серверу администрирования через шлюз соединений, который расположен в демилитаризованной зоне (DMZ). Обратный прокси-сервер и корпоративный сетевой экран не используются.

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

1. Сервер администрирования передает данные в базу данных. Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server и MariaDB Server или порт 5432 для PostgreSQL Server или Postgres Pro Server). Подробную информацию см. в документации СУБД.

2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000.

   Агенты администрирования отправляют запросы друг другу в пределах одного широковещательного домена. Затем данные отправляются на Сервер администрирования и используются для определения пределов широковещательного домена и для автоматического назначения точек распространения (если этот параметр включен).

   Если Сервер администрирования не имеет прямого доступа к управляемым устройствам, запросы на связь с Сервером администрирования на эти устройства не отправляются напрямую.

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

4. Сервер администрирования принимает подключения от Агентов администрирования и от подчиненных Серверов администрирования через TLS-порт 13000.

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

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

   Внешние устройства также подключаются к шлюзу соединения через TLS-порт 13000.

5. Управляемые устройства (кроме мобильных устройств) запрашивают активацию через TCP-порт 17000. В этом нет необходимости, если устройство имеет собственный доступ в интернет; в этом случае устройство отправляет данные на серверы "Лаборатории Касперского" напрямую через интернет.

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

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

7. Приложения на одном устройстве обмениваются локальным трафиком (либо на Сервере администрирования, либо на управляемом устройстве). Открывать внешние порты не требуется.

8. Данные от Сервера администрирования к серверам "Лаборатории Касперского" (например, данные KSN, информация о лицензиях) и данные от серверов "Лаборатории Касперского" к Серверу администрирования (например, обновления приложений и обновления антивирусных баз) передаются по протоколу HTTPS.

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

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

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

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

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

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

14. Только для мобильных устройств: управляемое приложение передает данные на Сервер администрирования (или на шлюз соединений) через TLS-порт 13292/13293 напрямую или через обратный прокси-сервер.

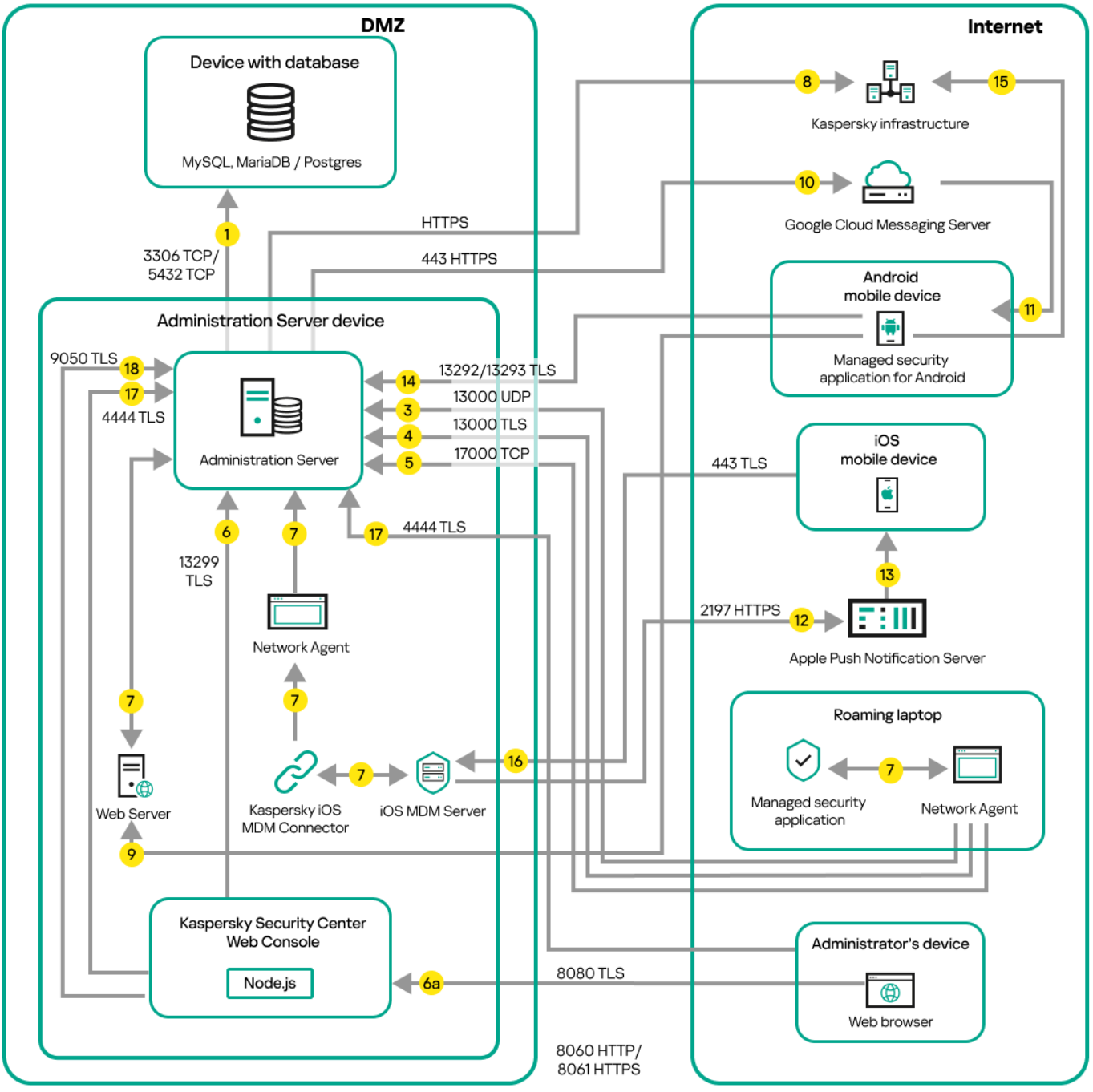
15. Только для мобильных устройств: данные от мобильного устройства передаются к инфраструктуре "Лаборатории Касперского".

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

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

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

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



Сервер администрирования в демилитаризованной зоне, управляемые мобильные устройства в интернете

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

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

1. Сервер администрирования передает данные в базу данных. Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server и MariaDB Server или порт 5432 для PostgreSQL Server или Postgres Pro Server). Подробную информацию см. в документации СУБД.

2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000.

   Агенты администрирования отправляют запросы друг другу в пределах одного широковещательного домена. Затем данные отправляются на Сервер администрирования и используются для определения пределов широковещательного домена и для автоматического назначения точек распространения (если этот параметр включен).

   Если Сервер администрирования не имеет прямого доступа к управляемым устройствам, запросы на связь с Сервером администрирования на эти устройства не отправляются напрямую.

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

4. Сервер администрирования принимает подключения от Агентов администрирования и от подчиненных Серверов администрирования через TLS-порт 13000.

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

5. Управляемые устройства (кроме мобильных устройств) запрашивают активацию через TCP-порт 17000. В этом нет необходимости, если устройство имеет собственный доступ в интернет; в этом случае устройство отправляет данные на серверы "Лаборатории Касперского" напрямую через интернет.

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

   Компонент Identity and Access Manager (IAM) подключается к Серверу администрирования по TLS-порту 13299.

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

7. Приложения на одном устройстве обмениваются локальным трафиком (либо на Сервере администрирования, либо на управляемом устройстве). Открывать внешние порты не требуется.

8. Данные от Сервера администрирования к серверам "Лаборатории Касперского" (например, данные KSN, информация о лицензиях) и данные от серверов "Лаборатории Касперского" к Серверу администрирования (например, обновления приложений и обновления антивирусных баз) передаются по протоколу HTTPS.

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

9. Запросы на пакеты от управляемых устройств передаются на Веб-сервер, который находится на том же устройстве, на котором установлен Сервер администрирования.

10. Только для мобильных устройств Android: данные от Сервера администрирования передаются серверам Google. Это соединение используется для уведомления мобильных устройств Android о том, что требуется их подключение к Серверу администрирования. Затем push-уведомления отправляются на мобильные устройства. Сервис FCM также работает на порту 443 HTTPS.

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

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

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

14. Только для мобильных устройств: управляемое приложение передает данные на Сервер администрирования (или на шлюз соединений) через TLS-порт 13292/13293 напрямую или через обратный прокси-сервер.

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

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

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

17. Сервер Kaspersky Security Center Web Console и браузер (используемый с Kaspersky Security Center Web Console) подключаются к Серверу администрирования по протоколу аутентификации OpenID Connect по TLS-порту 4444.

18. Сервер Kaspersky Security Center Web Console подключается к Серверу администрирования по TLS-порту 9050.

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

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

Условные обозначения в схемах взаимодействия

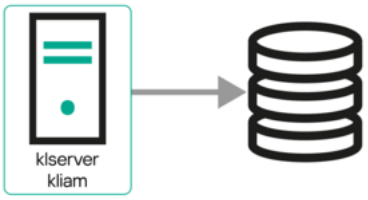
В таблице ниже приведены условные обозначения, использованные в схемах.

Условные обозначения

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

Сервер администрирования и СУБД

Данные Сервера администрирования и Identity and Access Manager (IAM) хранятся в разных базах данных одной СУБД.



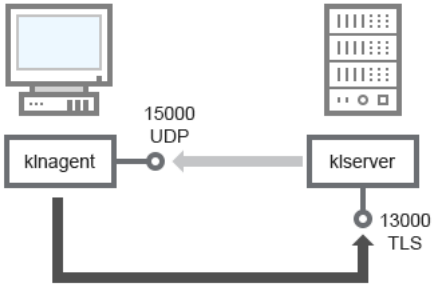
Сервер администрирования, Identity and Access Manager и СУБД

Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MariaDB). Подробную информацию см. в документации СУБД.
Порт для подключения IAM к СУБД задается пользователем при установке Kaspersky Security Center Linux.

Сервер администрирования не удаляет автоматически базу данных Сервера администрирования и базу данных IAM при удалении или переносе сервера на другое устройство. При необходимости вам нужно удалить базы вручную.

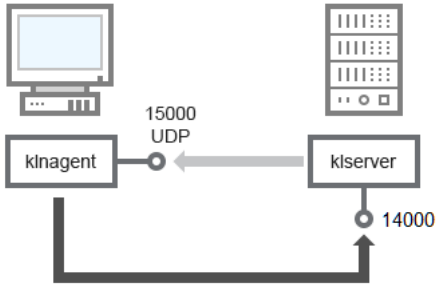
Сервер администрирования и клиентское устройство: Управление приложением безопасности

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



Сервер администрирования и клиентское устройство: управление приложением безопасности, подключение через порт 13000 (рекомендуется)

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



Сервер администрирования и клиентское устройство: управление приложением безопасности, подключение через порт 14000 (низкая защита)

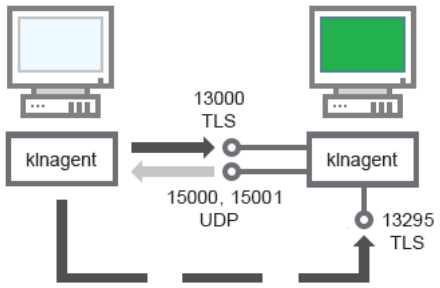
Пояснения к схемам см. в таблице ниже.

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

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

Обновление программного обеспечения на клиентском устройстве с помощью точки распространения

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



Обновление программного обеспечения на клиентском устройстве с помощью точки распространения

Пояснения к схеме см. в таблице ниже.

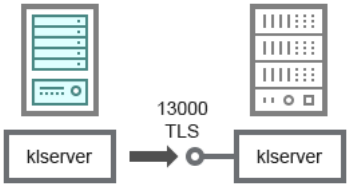
Обновление программного обеспечения с помощью точки распространения (трафик)

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

Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования

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

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



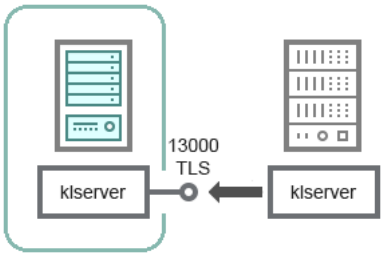
Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования

Пояснения к схеме см. в таблице ниже.

Иерархия Серверов администрирования (трафик)

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

Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне



Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне

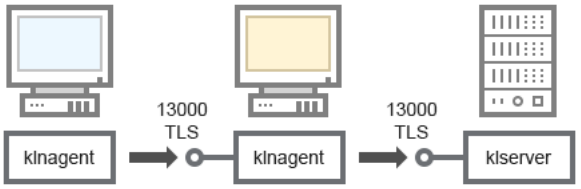
На схеме показана иерархия Серверов администрирования, в которой подчиненный Сервер, находящийся в демилитаризованной зоне, принимает подключение от главного Сервера (пояснения к схеме см. в таблице ниже). При объединении Серверов в иерархию необходимо, чтобы порт 13299 обоих Серверов был доступен. Приложение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

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

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

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

Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство



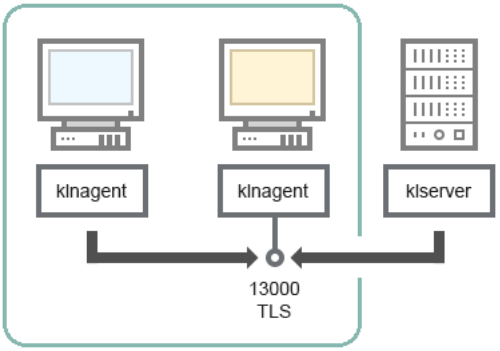
Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство

Пояснения к схеме см. в таблице ниже.

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

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

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



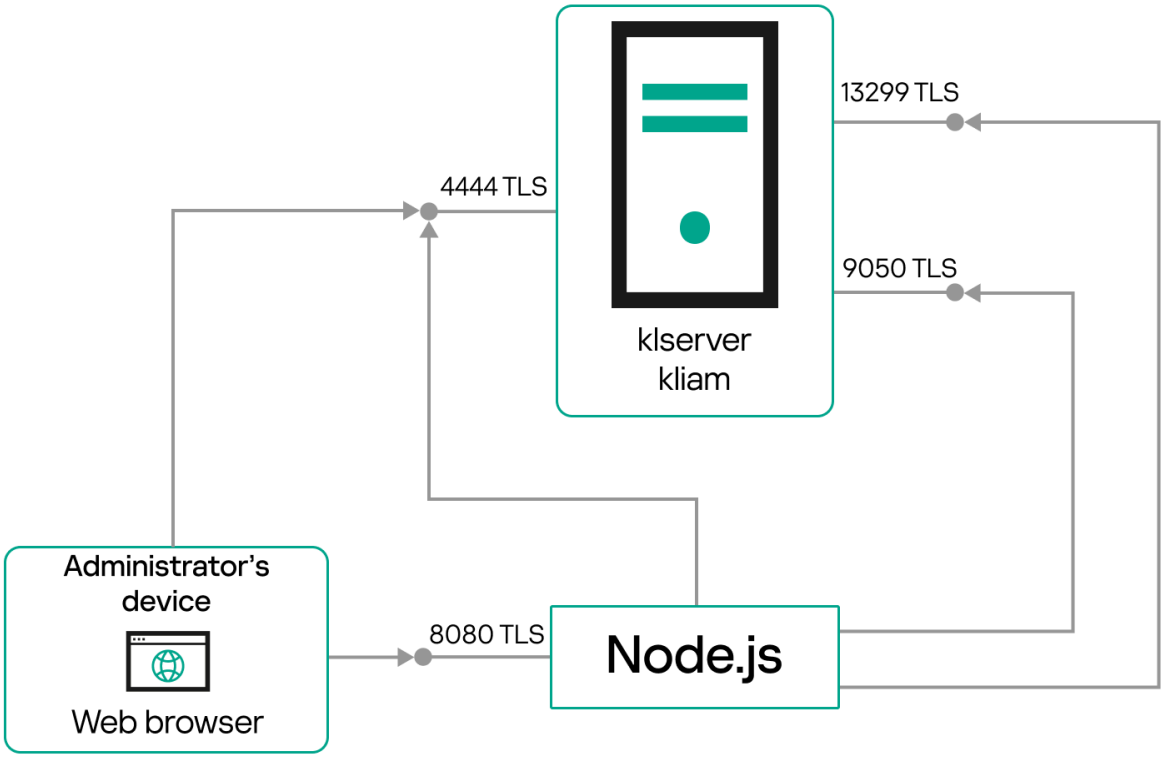
Сервер администрирования, шлюз соединений и клиентское устройство в демилитаризованной зоне

Пояснения к схеме см. в таблице ниже.

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

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

Сервер администрирования и Kaspersky Security Center Web Console



Сервер администрирования и Kaspersky Security Center Web Console

Пояснения к схеме см. в таблице ниже.

Сервер администрирования и Kaspersky Security Center Web Console (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта
Сервер администрирования	13299	klserver	TCP (TLS)	Прием подключений от Kaspersky Security Center Web Console и Identity and Access Manager (IAM) к Серверу администрирования по OpenAPI
Сервер Kaspersky Security Center Web Console или Сервер администрирования	8080	Node.js: серверный JavaScript	TCP (TLS)	Прием подключений от Kaspersky Security Center Web Console
Сервер администрирования	4444	kliam	TCP (TLS)	Прием подключений от Сервера Kaspersky Security Center Web Console и браузера (используется с Kaspersky Security Center Web Console) к Серверу администрирования с IAM по протоколу аутентификации OpenID Connect
Сервер администрирования	9050	kliam	TCP (TLS)	Прием подключений от Kaspersky Security Center Web Console к IAM

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

Начало работы

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

Предварительные требования

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

Если вы хотите попробовать Kaspersky Security Center 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. Воспользуйтесь рекомендациями для выбора структуры организации сети.

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.

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 Настройка сетевого доступа

Обеспечьте взаимодействие компонентов по сети организации согласно структуре защиты, выбранной на шаге 1.

Для этого вам нужно:

- открыть необходимые сетевые доступы;
- обеспечить подключение к серверам "Лаборатории Касперского" либо организовать обновление из другого источника обновлений;
- для подключения управляемых устройств к Серверу администрирования из интернета настроить доступ для работы через шлюзы соединения или разместить Сервер администрирования в демилитаризованной зоне.

4 Расчет оборудования и планирование установки компонентов

Если вы планируете устанавливать все компоненты Kaspersky Security Center Linux на одном сервере, используйте готовые расчеты характеристик оборудования из файла параметров скрипта быстрой установки (klfi_netsize). Убедитесь, что все требования по использованию автоматизированного скрипта развертывания компонентов подходят для вашей инфраструктуры.

В ином случае выполните полный расчет характеристик оборудования Сервера администрирования, СУБД и Web Console с учетом аппаратных и программных требований и раздела о расчетах аппаратных ресурсов для ручного развертывания решения по компонентам.

Для повышения уровня защищенности Kaspersky Security Center Linux включите в расчеты конфигураций аппаратные требования приложения Kaspersky Endpoint Security для Linux.

5 Установка компонентов Kaspersky Security Center Linux

Установите операционную систему, поддерживаемую Сервером администрирования и Kaspersky Security Center Web Console на целевых устройствах для развертывания решения.

Установите Kaspersky Security Center Linux в соответствии с запланированным типом развертывания:

- с помощью автоматизированного скрипта быстрой установки;
- согласно инструкции по ручной установке и настройке компонентов Сервера администрирования и Web Console.

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

По умолчанию приложение не использует устройство с Сервером администрирования как управляемое устройство. Для защиты Сервера администрирования и управления этим устройством следует 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.

Настройте параметры безопасности, необходимые для работы с Kaspersky Security Center Linux, в соответствии с рекомендациями в справке Kaspersky Endpoint Security для Linux.

Подробнее см. шаг "Настройка антивирусной защиты Сервера администрирования" в разделе Сценарий миграции на Kaspersky Security Center Linux с использованием скрипта быстрой установки.

7 Выполнение первоначальной настройки

При первом подключении к Серверу администрирования посредством Web Console автоматически запускается Мастер первоначальной настройки.

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.

8 Обнаружение сетевых устройств

Настройте и 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 приложения "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.

9 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.

10 Назначение точек распространения

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. Точки распространения для групп администрирования можно назначить автоматически либо вручную.

Назначить шлюзы соединений возможно только при использовании ручного режима назначения точек распространения.

Для этого:

- обеспечьте достаточное количество точек распространения после переключения режима назначения на ручной;
- сконфигурируйте необходимые подключения Сервера администрирования и шлюзов соединений до начала развертывания Агентов администрирования на устройствах сетевых местоположений, где устройства должны подключаться к Серверу администрирования через шлюзы соединений.

11 Установка Агента администрирования и приложений безопасности на устройства в сети

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

Чтобы выполнить удаленную установку приложений, запустите мастер развертывания защиты.

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

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

12 Распространение лицензионных ключей на клиентские устройства

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

13 Настройка политик приложений "Лаборатории Касперского"

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

14 Мониторинг состояния защиты сети

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

Долгосрочное хранение событий, оперативное получение событий, их обработка и корреляция должны производиться во внешней специализированной SIEM-системе.

Отслеживание показателей компонентов решения выполняется с использованием протокола SNMP в системах для мониторинга IT-инфраструктуры и иными сторонними агентскими решениями.

Постоянный контроль над состоянием защиты доступен в Web Console в разделе **Центр усиления защиты**.

Руководство по усилению защиты

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

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

Перед настройкой создайте резервную копию Сервера администрирования Kaspersky Security Center Linux с помощью задачи Резервное копирование данных Сервера администрирования или с помощью утилиты klbackup. Сохраните резервную копию данных в надежном месте.

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

Руководство по усилению защиты содержит следующую информацию:

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

- рекомендации по безопасности сторонних информационных систем.

Контрольный список по усилению защиты

Развертывание Сервера администрирования

- Установить Сервер администрирования на выделенный сервер (физический или виртуальный).
- Не использовать выделенный сервер в совместной работе с другими службами.
- Не устанавливать Сервер администрирования (далее также Сервер) на:
  - контроллер домена;
  - терминальный сервер;
  - пользовательское устройство.

Безопасность соединения

- Настроить сетевой экран, чтобы ограничить доступ к устройству Сервера по всем портам и протоколам, за исключением портов, требуемых Сервером. Разрешить доступ к устройству Сервера только с доверенных устройств.
- Настроить список разрешенных IP-адресов для портов Сервера, используемых для подключения Kaspersky Security Center Web Console (далее также Web Console) к Серверу.
- Настроить сетевой экран – разрешить доступ к Серверу через Web Console только с доверенных устройств.
- Настроить протокол TLS 1.2 или выше на Сервере.
- Настроить сетевой экран для ограничения доступа к устройству с установленной СУБД Сервера.
- Настроить SSL-аутентификацию между Сервером и СУБД (MySQL или PostgreSQL).

Учетные записи и авторизация

- Настроить двухфакторную аутентификацию (TOTP, RFC 6238) для доступа к Серверу.
- Не устанавливать приложение для аутентификации на устройство, с которого выполняется подключение к Серверу через Web Console.
- Для доступа к устройству с Сервером использовать многофакторную аутентификацию (MFA) – токен, смарт-карту или другой способ.

- Создать выделенную группу администрирования для устройства Сервера с отдельной политикой безопасности.
- Ограничить количество пользователей с ролью Главный администратор.
- Настроить права доступа к функциям Сервера на основе ролей для пользователей и групп.
- Разрешить удаленную установку приложений только для другой выделенной учетной записи пользователя.
- Проводить регулярный аудит пользователей на устройстве Сервера.

Управление защитой Сервера администрирования

- Установить приложение безопасности на устройство с Сервером:
  - на физический сервер – Kaspersky Endpoint Security;
  - на виртуальный сервер – Kaspersky Security для виртуальных сред.
- Создать и применить отдельную политику для приложения безопасности, защищающего Сервер (отличную от клиентских политик для других управляемых устройств).
- Создать и применить отдельный пароль для приложения безопасности, защищающего Сервер (отличный от паролей для других управляемых устройств).
- Включите все доступные модули защиты в приложении безопасности (информацию о параметрах безопасности, необходимых для работы с Сервером администрирования, см. в справке Kaspersky Endpoint Security для Linux).

Настройка политик и задач управляемых приложений

- Создать и применить политики ко всем управляемым устройствам или к группе новых устройств для используемых приложений:
  - Агент администрирования;
  - Kaspersky Endpoint Security для Windows/Linux/macOS;
  - Kaspersky Endpoint Agent (или другие приложения "Лаборатории Касперского").
- Включить защиту паролем от выключения или удаления приложений "Лаборатории Касперского".
- Заблокировать параметры политики (закрыть значок замка), чтобы предотвратить переназначение этих параметров на управляемых устройствах.
- Создать регулярную задачу полной проверки устройств.
- Включить Kaspersky Security Network (KSN) и принять актуальные положения KSN.

- Настроить обнаружение устройств и указать группу администрирования по умолчанию, в которую попадают все новые обнаруженные устройства.
- Ограничить использование автоматических правил перемещения устройств между группами администрирования.
- Защитить точки распространения от несанкционированного доступа.
- Избегать автоматического назначения точек распространения в небольших и критичных сетях.

Обслуживание Сервера администрирования

- Не удалять и не выключать задачи:
  - резервного копирования;
  - обслуживания Сервера.
- Своевременно устанавливать обновления ОС и стороннего программного обеспечения.

Передача событий в сторонние системы

- Настроить мониторинг и рассылку отчетов о событиях безопасности.
- Настроить передачу событий в SIEM-систему.
- Настроить отправку уведомлений Сервера о:
  - событиях аудита;
  - критических событиях;
  - сбоях и предупреждениях.

Рекомендации по безопасности сторонних информационных систем

- Применять рекомендации по безопасности CIS Benchmarks к используемым ОС, СУБД, гипервизорам.
- Для Astra Linux – использовать рекомендации из Red Book соответствующей версии.
- Для РЕД ОС – использовать рекомендации из официальной документации РЕД ОС.

Развертывание Сервера администрирования

Архитектура Сервера администрирования

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

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

На основании этой информации нужно сформировать архитектуру, определяющую:

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

Выбор устройства для Сервера администрирования

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

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

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

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

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

Учетные записи для установки и запуска Сервера администрирования

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

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

Набор необходимых учетных записей и их прав зависит от выбранного типа СУБД и способа создания базы данных Сервера администрирования.

Безопасность соединения

Использование TLS

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

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

Строгие параметры TLS

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

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

Ограничение доступа к базе данных Сервера администрирования

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

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

Безопасность взаимодействия с внешней СУБД

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

Настройка списка разрешенных IP-адресов для подключения к Серверу администрирования

По умолчанию пользователи Kaspersky Security Center Linux могут войти в Kaspersky Security Center Linux с любого устройства, на котором установлено приложение Kaspersky Security Center Web Console или приложение OpenAPI. Настроить Сервер администрирования можно таким образом, чтобы пользователи могли подключаться к нему только с устройств с разрешенными IP-адресами. Например, если злоумышленники попытаются подключиться к Kaspersky Security Center Linux через Сервер Kaspersky Security Center Web Console, установленный на устройстве, которое не включено в список разрешенных, они не смогут войти в Kaspersky Security Center Linux.

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

По умолчанию пользователи Kaspersky Security Center Linux могут подключаться к Kaspersky Security Center Web Console с любого устройства. На устройстве с Kaspersky Security Center Web Console необходимо настроить сетевой экран (встроенный в операционную систему или сторонний) таким образом, чтобы пользователи могли подключаться к Kaspersky Security Center Web Console только с разрешенных IP-адресов.

Безопасное подключение к контроллеру домена во время опроса

Чтобы опросить контроллер домена, Сервер администрирования или точка распространения с операционной системой Linux пытается подключиться к этому домену через LDAP. По умолчанию проверка сертификата при подключении не требуется. Чтобы принудительно включить проверку сертификата, нужно установить для флага `KLNAG_LDAP_TLS_REQCERT` значение 1. Вы также можете указать путь к сертификату от аккредитованного центра сертификации (CA) для доступа к цепочке сертификатов, используя флаг `KLNAG_LDAP_SSL_CACERT`.

Учетные записи и авторизация

Перед выполнением шагов ниже, создайте резервную копию данных Сервера администрирования Kaspersky Security Center Linux с помощью задачи Резервное копирование данных Сервера администрирования или с помощью утилиты klbackup. Сохраните резервную копию данных в надежном месте.

Использование двухфакторной аутентификации Сервера администрирования

В Kaspersky Security Center Linux для входа в Kaspersky Security Center Web Console используется **двухфакторная аутентификация** в соответствии со стандартом RFC 6238 (TOTP: Time-Based One-Time Password algorithm – алгоритм временных одноразовых паролей).

При каждом входе в Kaspersky Security Center Web Console пользователь вводит свое имя пользователя, пароль и дополнительный одноразовый код безопасности. Для получения одноразового кода безопасности на компьютере или мобильном устройстве пользователя должно быть установлено приложение для аутентификации.

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

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

Использование двухфакторной аутентификации операционной системы

Для обеспечения комплексной защиты с помощью двухфакторной аутентификации должна быть обеспечена безопасность не только Сервера администрирования, но и устройства, на котором Сервер установлен.

При подключении к устройству, на котором установлен Сервер администрирования (по SSH, RDP или другому протоколу), рекомендуется использовать многофакторную аутентификацию (MFA) с помощью токена, смарт-карты или другого метода аутентификации.

Запрет на сохранение пароля администратора

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

Авторизация внутреннего пользователя

По умолчанию пароль внутренней учетной записи пользователя Сервера администрирования должен соответствовать следующим требованиям:

- Длина пароля должна быть от 8 до 256 символов.
- Пароль должен содержать символы как минимум трех групп из 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 "@".

По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить количество попыток ввода пароля.

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

Настройка параметров смены пароля внутренней учетной записи пользователя

Рекомендуется настроить следующие параметры для изменения пароля внутренней учетной записи пользователя:

- Период смены пароля.
- Время предварительного предупреждения о необходимости смены пароля.
- Параметр **Пользователю нужно сменить пароль при первом входе**.

Защита учетной записи от несанкционированного изменения

Рекомендуется включить дополнительный параметр для защиты внутренней учетной записи пользователя Сервера администрирования от несанкционированного изменения. Эту защиту необходимо настраивать отдельно для каждого внутреннего пользователя.

Отдельная группа администрирования для устройства с Сервером администрирования

Для Сервера администрирования

рекомендуется создать выделенную группу администрирования. Предоставьте этой группе особые права доступа и создайте для нее специальную политику безопасности.

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

Ограничение назначения роли Главного администратора

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

Настройка прав доступа к функциям приложения

Рекомендуется использовать возможности гибкой настройки прав доступа пользователей и групп пользователей к разным функциям Kaspersky Security Center Linux.

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

Основные преимущества ролевой модели управления доступом:

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

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

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

- Управление группами администрирования.
- Операции с Сервером администрирования.
- Удаленная установка.

- Изменение параметров хранения событий и отправки уведомлений.

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

Отдельная учетная запись для удаленной установки приложений

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

Рекомендуется использовать отдельную учетную запись для удаленной установки приложений. Вы можете назначить роль или разрешения отдельной учетной записи.

Регулярный аудит всех пользователей и их действий

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

Также вы можете отслеживать действия пользователей, такие как подключение к Серверу администрирования и отключение от него, подключение к Серверу администрирования с ошибкой и изменение объектов (для объектов, поддерживающих управление версиями).

Управление защитой Сервера администрирования

Выбор приложения защиты Сервера администрирования

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

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

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

- Kaspersky Industrial CyberSecurity for Nodes. Это приложение рекомендуется устанавливать на устройства, входящие в промышленную сеть. Kaspersky Industrial CyberSecurity for Nodes – это приложение, имеющее сертификаты совместимости с различными производителями промышленного программного обеспечения.

- Рекомендованные приложения безопасности. Если Сервер администрирования установлен на устройство с другим программным обеспечением, нужно ознакомиться с рекомендациями производителя программного обеспечения по использованию антивирусных приложений (возможно, уже существуют рекомендации по выбору приложения защиты, и, вероятно, вам потребуется выполнить настройку доверенной зоны).

Создание отдельной политики безопасности для защиты приложения

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

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

Модули защиты

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

Настройка сетевого экрана устройства с Сервером администрирования

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

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

Управление защитой Агента администрирования

Чтобы злоумышленники не могли вывести устройства из-под контроля вашего Сервера администрирования, мы настоятельно рекомендуем придерживаться описанных практик.

Использование пароля деинсталляции

В параметрах инсталляционного пакета Агента администрирования задайте пароль деинсталляции, которой будет запрашиваться при удалении Агента администрирования.

Функциональность доступна только для Агента администрирования на устройствах под управлением операционной системы семейства Windows.

Использование усиленной защиты Агента администрирования

В параметрах инсталляционного пакета Агента администрирования включите параметр **Защитить службу Агента администрирования от неавторизованного удаления, остановки или изменения параметров работы**. После того как Агент администрирования установлен на управляемом устройстве, компонент невозможно удалить или изменить без требуемых прав. Работа Агента администрирования не может быть остановлена.

Функциональность доступна только для Агента администрирования на устройствах под управлением операционной системы семейства Windows.

Отслеживание адреса Сервера администрирования, к которому подключается Агент администрирования

Для отслеживания несанкционированного переключения Агента администрирования на внешний Сервер администрирования используйте Kaspersky Event Log. Kaspersky Event Log – это раздел журнала событий, который хранится в операционной системе управляемых устройств. В Windows содержимое журнала можно посмотреть с помощью Event Viewer, в Linux – с помощью утилиты journalctl.

При подключении Агента администрирования к Серверу администрирования в Kaspersky Event Log регистрируются одна или две записи, содержащие следующую информацию:

- Адрес Сервера администрирования:
  - **Try to connect to Administration Server at <Administration Server address>**.
  - **Connected to Administration Server at <Administration Server address>**.
- Адрес Сервера администрирования и шлюза соединения при подключении через шлюз:
  - **Try to connect to Administration Server at <Administration Server address> via CG <connection gateway address>**.
  - **Connected to Administration Server at <Administration Server address> via CG <connection gateway address>**.

Событие с адресом Сервера администрирования регистрируется в следующих случаях:

- при каждом перезапуске службы Агента администрирования;
- при подключении Агента администрирования к другому Серверу администрирования;
- раз в сутки при штатной работе устройства, даже если служба Агента администрирования не перезапускалась и Агент администрирования не подключался к другому Серверу администрирования (в этом случае в журнале повторно опубликуется только первая запись).

Для удобства рекомендуем настроить выгрузку событий из Kaspersky Event Log в SIEM-систему и формировать алерт, если указанный в событии адрес Сервера администрирования не совпадает с текущим адресом вашего Сервера администрирования.

Чтобы настроить выгрузку событий из Kaspersky Event Log:

1. В SIEM-системе настройте получение событий из Kaspersky Event Log со всех управляемых устройств.
2. Создайте правило корреляции, срабатывающее при получении события о смене Сервера администрирования, к которому подключается Агент администрирования.
3. Настройте создание алерта при срабатывании этого правила корреляции.
4. При необходимости настройте отправку уведомлений об алерте на электронную почту или создайте в панели мониторинга виджет с информацией об алертах.

Управление защитой клиентских устройств

Ограничение добавления лицензионных ключей в инсталляционные пакеты

Инсталляционные пакеты хранятся в папке общего доступа Сервера администрирования, во вложенной папке Packages. Если вы добавите лицензионный ключ в инсталляционный пакет, лицензионный ключ будет доступен всем пользователям с правами чтения в этой папке (напрямую или через Веб-сервер, встроенный в Сервер администрирования).

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

Рекомендуется использовать автоматическое распространение лицензионных ключей на управляемые устройства, выполнять развертывание с помощью задачи Добавление лицензионного ключа для управляемого приложения, и добавлять код активации или файл ключа на устройства вручную.

Правила автоматического перемещения устройств между группами администрирования

Рекомендуется ограничить использование правил автоматического перемещения устройств между группами администрирования.

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

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

Эта рекомендация, не относится к первоначальному распределению устройств по группам администрирования.

Требования безопасности к устройствам с точками распространения и шлюзам соединений

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

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

Размещение точек распространения в сети организации используется для следующих задач:

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

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

Ограничение автоматического назначения точек распространения

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

В промышленных и небольших сетях вы можете назначить точки распространения вручную.

При необходимости вы также можете просмотреть Отчет о работе точек распространения.

Требования безопасности к устройствам пользователей Kaspersky Security Center Linux

К устройствам пользователей Kaspersky Security Center Linux должны применяться особые требования безопасности. Рекомендуется защитить эти устройства от любого вида несанкционированного доступа, в том числе физического.

К устройствам пользователей Kaspersky Security Center Linux относятся следующие устройства:

- Устройства, с которых пользователи Kaspersky Security Center Linux подключаются к Kaspersky Security Center Web Console с помощью браузера.
- Устройства, с которых приложения подключаются к Kaspersky Security Center Linux, взаимодействующие с Сервером администрирования через OpenAPI.

Требования безопасности к устройствам с установленным приложением Kaspersky Security Center Web Console

Для управления Kaspersky Security Center Linux используются устройства с установленным приложением Kaspersky Security Center Web Console, поэтому к безопасности таких устройств предъявляются особые требования. Рекомендуется защитить эти устройства от любого вида несанкционированного доступа, в том числе физического.

Настройка защиты управляемых приложений

Политики управляемых приложений

Рекомендуется создать политику для каждого вида используемых приложений и компонентов Kaspersky Security Center Linux (Агент администрирования, Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Agent и другие). Эта групповая политика должна применяться ко всем управляемым устройствам (корневой группе администрирования) или к отдельной группе, в которую автоматически попадают новые управляемые устройства в соответствии с настроенными правилами перемещения.

Установка пароля на выключение защиты и удаление приложения

Настоятельно рекомендуется включить защиту паролем, чтобы злоумышленники не смогли выключить или удалить приложения безопасности "Лаборатории Касперского". На платформах, где поддерживается защита паролем, вы можете установить пароль, например, для Kaspersky Endpoint Security, Агента администрирования и других приложений "Лаборатории Касперского". После включения защиты паролем рекомендуется заблокировать соответствующие параметры, закрыв их "замком".

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

Утилита klmover позволяет вручную подключить клиентское устройство к Серверу администрирования. Утилита klmover находится в папке установки Агента администрирования.

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

Утилита klmover требует прав локального администратора.

Если вы потеряли или забыли пароль от Агента администрирования, установленного на устройстве и защищенного паролем, которое больше не находится под управлением Kaspersky Security Center Linux, вы не сможете удалить этот Агент администрирования с помощью утилиты klmover или с помощью командной строки. В этом случае необходимо переустановить операционную систему на устройстве с установленным Агентом администрирования, защищенным паролем.

При включении параметра **Использовать пароль деинсталляции** на устройствах с операционной системой Windows также включается защита паролем средствами Cleaner (cleaner.exe).

Использование Kaspersky Security Network

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

Регулярная проверка управляемых устройств

Для всех групп устройств вам нужно создать задачу, периодически запускающую полную проверку устройств.

Обнаружение новых устройств

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

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

Обслуживание Сервера администрирования

Резервное копирование данных Сервера администрирования

Резервное копирование данных позволяет восстановить данные Сервера администрирования без их потери.

По умолчанию задача резервного копирования создается автоматически после установки Сервера администрирования и выполняется периодически с сохранением резервных копий в соответствующей директории.
Пользователь может изменить параметры задачи резервного копирования:

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

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

Обслуживание Сервера администрирования

Обслуживание Сервера администрирования позволяет сократить объем базы данных, повысить производительность и надежность работы приложения. Рекомендуется обслуживать Сервер администрирования не реже раза в неделю.

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

- перестраивает индексы базы данных;
- обновляет статистику базы данных;
- сжимает базу данных (при необходимости).

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

Настоятельно рекомендуется регулярно выполнять установку обновлений операционной системы и стороннего программного обеспечения на устройстве с Сервером администрирования.

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

Передача событий в сторонние системы

Мониторинг и отчеты

Для своевременного реагирования на проблемы безопасности вы можете настроить функции мониторинга и параметры отчетов.

Экспорт событий в SIEM-системы

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

Уведомление по электронной почте о событиях аудита

Kaspersky Security Center Linux позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Для своевременного реагирования на возникновение нештатных ситуаций рекомендуется настроить отправку Сервером администрирования уведомлений о публикуемых им событиях аудита, критических событиях, событиях отказа функционирования и предупреждениях.

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

Рекомендации по безопасности сторонних информационных систем

Рекомендации по безопасности CIS Benchmarks

При использовании версий операционных систем, платформ виртуализации или серверов баз данных, поддерживаемых Сервером администрирования и Агентом администрирования, для тонкой настройки этих информационных систем рекомендуется применять методы защиты информации Center for Internet Security (CIS), если они существуют.

Center for Internet Security (CIS) – некоммерческая организация, занимающаяся повышением безопасности в области информационных технологий. В частности, CIS разрабатывает и распространяет стандарты безопасности, такие как CIS Controls и CIS Benchmarks. Эти стандарты представляют собой набор рекомендаций и практик по обеспечению безопасности информационных систем.

На портале CIS есть рекомендации для версий следующих информационных систем, поддерживаемых Сервером администрирования и Агентом администрирования:

- Операционные системы следующих семейств:
  - Windows для рабочих станций
  - Windows для серверов
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS
- Платформы виртуализации VMware
- Серверы баз данных:
  - Microsoft SQL Server
  - MySQL
  - MariaDB
  - PostgreSQL

Рекомендации по безопасности для операционной системы Astra Linux

При использовании операционной системы Astra Linux следует соблюдать рекомендации по безопасности, описанные в Red Book для соответствующей версии Astra Linux.

Рекомендации по безопасности для операционной системы РЕД ОС

При использовании операционной системы РЕД ОС необходимо следовать рекомендациям по безопасности из руководства администратора, приведенным в официальной документации РЕД ОС.

Рекомендации по использованию приложений безопасности "Лаборатории Касперского"

Использование пароля KLAdmin в Kaspersky Endpoint Security для Windows

Учетная запись KLAdmin – это учетная запись администратора с неограниченным доступом к приложению Kaspersky Endpoint Security для Windows. Учетная запись KLAdmin имеет право выполнять любое действие, защищенное паролем, в Kaspersky Endpoint Security для Windows, включая удаление приложения. Права для учетной записи KLAdmin не могут быть отозваны. Вы можете установить пароль для учетной записи KLAdmin в свойствах политики Kaspersky Endpoint Security для Windows. Администратор Kaspersky Endpoint Security для Windows несет полную ответственность за безопасное использование пароля для учетной записи KLAdmin. Если в вашей организации есть собственная политика использования паролей, следуйте указаниям этой политики. Чем длиннее и сложнее пароль, тем он надежнее.

Чтобы защитить организацию от кражи пароля KLAdmin, выполните следующие действия:

- **Общие требования.**

  Не используйте имя учетной записи или часть имени в качестве пароля.

- **Требования к минимальной длине пароля.**

  Создайте пароль, который содержит не менее 10 символов.

- **Требования использования нескольких типов символов.**

  Задайте комплексный пароль, который содержит символы из разных категорий: буквы нижнего и верхнего регистров, цифры и специальные символы.

- **Требования к сроку действия пароля.**

  Установите минимальный срок действия пароля в 90 дней. Новый пароль не должен совпадать ни с одним из последних 24 паролей.

Сценарий: аутентификация MySQL Server

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

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

Включение односторонней SSL-аутентификации

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

1. **Создайте самоподписанный TLS-сертификат для сервера MySQL**

Выполните следующую команду:

```
openssl genrsa 1024 > ca-key.pem

openssl req -new -x509 -nodes -days 365 -key ca-key.pem -config myssl.cnf > ca-cert.pem

openssl req -newkey rsa:1024 -days 365 -nodes -keyout server-key.pem -config myssl.cnf
> server-req.pem

openssl x09 -req -in server-req.pem -days 365 -CA ca-cert.pem -CAkey ca-key.pem -
set_serial 01 > server-cert.pem
```

2. **Создайте файл флага сервера**

   С помощью утилиты klscflag создайте флаг сервера KLSRV_MYSQL_OPT_SSL_CA и укажите путь к сертификату в качестве его значения. Утилита klscflag находится в директории, в которой установлен Сервер администрирования. По умолчанию задан путь /opt/kaspersky/ksc64/sbin.

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <path to ca-cert.pem> -t d
   ```

3. **Настройте базу данных**

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

   ```
   [mysqld]

   ssl-ca=".../mysqlcerts/ca-cert.pem"

   ssl-cert=".../mysqlcerts/server-cert.pem"

   ssl-key=".../mysqlcerts/server-key.pem"
   ```

Включение двусторонней SSL-аутентификации

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

1. **Создайте файлы флага сервера**

   С помощью утилиты klscflag создайте флаги сервера и укажите путь к файлам сертификатов в качестве их значений:

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <path to ca-cert.pem> -t s

   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <path to server-cert.pem> -t
   s

   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <path to server-key.pem> -t s
   ```

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

2. **Укажите парольную фразу (необязательно)**

   Если server-key.pem требует кодовую фразу, создайте флаг KLSRV_MARIADB_OPT_TLS_PASPHRASE и укажите кодовую фразу в качестве его значения:

   ```
   klscflag -fset -pv klserver -n KLSRV_MARIADB_OPT_TLS_PASPHRASE -v <passphrase> -t s
   ```

3. **Настройте базу данных**

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

```
[mysqld]
ssl-ca=".../mysqlcerts/ca-cert.pem"
ssl-cert=".../mysqlcerts/server-cert.pem"
ssl-key=".../mysqlcerts/server-key.pem"
```

Сценарий: двухсторонняя TLS-аутентификация PostgreSQL для базы данных Сервера администрирования и базы данных IAM

В Kaspersky Security Center Linux вы можете настроить шифрование и взаимную проверку сертификатов между сервером PostgreSQL и клиентами – Сервером администрирования и IAM. Для каждой базы данных используется отдельный пользователь и отдельный клиентский сертификат. Кроме TLS применяется парольная аутентификация `scram-sha-256`.

Аутентификация сервера PostgreSQL состоит из следующих этапов:

1. **Подготовка СУБД и создание ролей**

   Выполните следующие команды:

   ```
   sudo -u postgres psql
   CREATE DATABASE kav;
   CREATE DATABASE iam;
   CREATE USER myuserksc WITH PASSWORD '*password*';
   ALTER ROLE myuserksc WITH LOGIN CREATEDB;
   ALTER DATABASE kav OWNER TO myuserksc;
   CREATE USER myuseriam WITH PASSWORD '*password*';
   ALTER ROLE myuseriam WITH LOGIN CREATEDB;
   ALTER DATABASE iam OWNER TO myuseriam;
   ```

2. **Создание собственного CA и серверного сертификата (односторонняя SSL-аутентификация)**

   `subjectAltName` (SAN) – обязательный параметр в серверном сертификате. Значение параметра должно соответствовать FQDN хоста.

   Выполните следующие команды:

   ```
   sudo openssl req -x509 -nodes -newkey rsa:4096 -keyout /etc/ssl/private/postgresql_ca.key -out
   /etc/ssl/certs/postgresql_ca.crt -days 365 -addext "subjectAltName=DNS:*FQDN*" -subj "/CN=mysrvca"
   sudo openssl req -new -nodes -newkey rsa:4096 -keyout /etc/ssl/private/postgresql_leaf.key -out
   /tmp/postgresql_leaf.csr -addext "subjectAltName=DNS:< FQDN >" -subj "/CN=*FQDN*"
   sudo openssl x509 -req -in /tmp/postgresql_leaf.csr -CA /etc/ssl/certs/postgresql_ca.crt -CAkey
   /etc/ssl/private/postgresql_ca.key -CAcreateserial -out /etc/ssl/certs/postgresql_leaf.crt -days 365 -sha256 -
   copy_extensions copy
   sudo cat /etc/ssl/certs/postgresql_leaf.crt /etc/ssl/certs/postgresql_ca.crt | sudo tee
   /etc/ssl/certs/postgresql.crt
   sudo chmod 600 /etc/ssl/private/postgresql_leaf.key
   sudo chown postgres:postgres /etc/ssl/private/postgresql_leaf.key
   sudo chmod 644 /etc/ssl/certs/postgresql_leaf.crt
   sudo chown ksc:kladmins /etc/ssl/certs/postgresql_ca.crt
   sudo chmod 644 /etc/ssl/certs/postgresql_ca.crt
   sudo chmod 644 /etc/ssl/certs/postgresql.crt
   ```

3 Создание клиентского CA и сертификатов для базы данных Сервера администрирования и базы данных IAM (двусторонняя SSL-аутентификация)

Выполните следующие команды:

```
sudo openssl req -x509 -nodes -newkey rsa:4096 -keyout /etc/ssl/private/postgresql_cli_ca.key -out
/etc/ssl/certs/postgresql_cli_ca.crt -days 365 -subj "/CN=myclica"
openssl x509 -in /etc/ssl/certs/postgresql_cli_ca.crt -text -noout
sudo chmod 600 /etc/ssl/private/postgresql_cli_ca.key
sudo chmod 644 /etc/ssl/certs/postgresql_cli_ca.crt
openssl req -new -nodes -newkey rsa:4096 -keyout $HOME/postgresql_cli_myuserksc.key -out
/tmp/postgresql_cli_myuserksc.csr -subj "/CN=myuserksc"
sudo openssl x509 -req -in /tmp/postgresql_cli_myuserksc.csr -CA /etc/ssl/certs/postgresql_cli_ca.crt -CAkey
/etc/ssl/private/postgresql_cli_ca.key -CAcreateserial -out $HOME/postgresql_cli_myuserksc.crt -days 365
openssl req -new -nodes -newkey rsa:4096 -keyout $HOME/postgresql_cli_myuseriam.key -out
/tmp/postgresql_cli_myuseriam.csr -subj "/CN=myuseriam"
sudo openssl x509 -req -in /tmp/postgresql_cli_myuseriam.csr -CA /etc/ssl/certs/postgresql_cli_ca.crt -CAkey
/etc/ssl/private/postgresql_cli_ca.key -CAcreateserial -out $HOME/postgresql_cli_myuseriam.crt -days 365
```

4 Копирование клиентских сертификатов на хост Сервера администрирования и IAM и установка прав

Выполните следующие команды:

```
sudo cp $HOME/postgresql_cli_myuserksc.crt   /home/ksc/
sudo cp $HOME/postgresql_cli_myuserksc.key   /home/ksc/
sudo cp $HOME/postgresql_cli_myuseriam.crt   /home/ksciam/
sudo cp $HOME/postgresql_cli_myuseriam.key   /home/ksciam/
sudo chown ksc:kladmins /home/ksc/*.crt /home/ksc/*.key
sudo chown ksciam:kladmins /home/ksciam/*.crt /home/ksciam/*.key
sudo chmod 644 /home/ksc/*.crt
sudo chmod 600 /home/ksc/*.key
sudo chmod 644 /home/ksciam/*.crt
sudo chmod 600 /home/ksciam/*.key
```

5 Настройка PostgreSQL

Измените файл postgresql.conf следующим образом:

```
listen_addresses = '*'
ssl = on
ssl_cert_file = '*path to postgresql.crt*'
ssl_key_file = '*path to postgresql_leaf.key*'
ssl_ca_file = '*path to postgresql_cli_ca.crt*'
```

Измените файл pg_hba.conf следующим образом:

```
hostssl    kav    myuserksc    *Administration Server IP address*    scram-sha-256    clientcert=verify-full
hostssl    iam    myuseriam    *Administration Server IP address*    scram-sha-256    clientcert=verify-full
```

Если Сервер администрирования и PostgreSQL находятся на одном устройстве, используйте адрес `127.0.0.1/32` и `listen_addresses = 'localhost'`.

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

6 Перезапуск демона PostgreSQL

Выполните следующую команду:

```
systemctl restart postgresql
```

7 Задание флага сервера для Сервера администрирования

С помощью утилиты klscflag создайте флаги сервера и укажите путь к файлам сертификатов в качестве их значений.

Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: `/opt/kaspersky/ksc64/sbin/`.

Выполните следующие команды:

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v *path to postgresql_cli_myuserksc.crt* -t s
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v *path to postgresql_cli_myuserksc.key* -t s
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v *path to postgresql_ca.crt* -t s
```

Если postgres_leaf.key требует кодовую фразу, создайте флаг `KLSRV_POSTGRES_OPT_TLS_PASPHRASE` и укажите кодовую фразу в качестве его значения:

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v *pasphrase* -t s
```

8. **Настройка IAM**

   Измените файл iam_config.yaml следующим образом:

   ```
   dbms_tl_opt_ssl_ca: "/etc/ssl/certs/postgresql_ca.crt"
   dbms_tl_opt_ssl_verify_server_cn: "1"
   dbms_tl_opt_ssl_cert: "/home/ksc/postgresql_cli_myuseriam.crt"
   dbms_tl_opt_ssl_key:  "/home/ksc/postgresql_cli_myuseriam.key"
   ```

9. **Перезапуск служб Сервера администрирования**

   Выполните следующую команду:

   ```
   sudo systemctl restart kl*
   ```

Подготовка к развертыванию

В этом разделе описывается, как выбрать вариант развертывания Kaspersky Security Center Linux и как выполнить настройку Kaspersky Security Center Linux и СУБД в соответствии с требованиями вашей организации.

Есть несколько вариантов развертывания компонентов Kaspersky Security Center Linux в сети организации в зависимости от следующих критериев:

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

Один Сервер администрирования может обслуживать до 50 000 устройств (с PostgreSQL или Postgres Pro в качестве СУБД). Если общее количество устройств в сети организации превышает 50 000, следует разместить в сети организации несколько Серверов администрирования, объединенных в иерархию для удобства централизованного управления.

Если в составе организации есть крупные географически удаленные офисы (филиалы) с собственными администраторами, целесообразно разместить в этих офисах Серверы администрирования. В ином случае такие офисы следует рассматривать как обособленные сети, связанные узкими каналами, см. статью "Типовая конфигурация: несколько крупных офисов с собственными администраторами".

При наличии обособленных сетей, связанных узкими каналами, в целях экономии трафика в таких сетях следует назначить один или несколько Агентов администрирования точками распространения (см. таблицу для расчета количества точек распространения). В этом случае все устройства обособленной сети будут получать обновления с таких "локальных центров обновлений". Точки распространения могут загружать обновления как с Сервера администрирования (поведение по умолчанию), так и с размещенных в интернете серверов "Лаборатории Касперского", см. статью "Типовая конфигурация: множество небольших изолированных офисов".

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

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

- для инспекции SSL трафика посредством SSL termination proxy или для использования Reverse Proxy;
- для интеграции с инфраструктурой открытых ключей (PKI) организации;
- для задания желательных значений полей сертификата;
- для обеспечения желаемой криптографической стойкости сертификата.

Выбор конфигурации Kaspersky Security Center Linux

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

- Один офис.
- Несколько крупных географически распределенных офисов с собственными администраторами.
- Множество небольших географически распределенных офисов.

Типовая конфигурация: один офис

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

Один Сервер администрирования может обслуживать не более чем 50 000 устройств (с PostgreSQL или Postgres Pro в качестве СУБД). Нужно учесть возможность увеличения количества управляемых устройств в ближайшем будущем: может оказаться желательным подключение несколько меньшего количества устройств к одному Серверу администрирования.

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

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

Типовая конфигурация: несколько крупных офисов с собственными администраторами

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

При наличии сотрудников, которые перемещаются между офисами вместе с устройствами (ноутбуками), в политике Агента администрирования следует создать профили подключения Агента администрирования.

Типовая конфигурация: множество небольших удаленных офисов

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

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

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

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

Сервер администрирования не сможет посылать уведомления на порт 15000 UDP управляемым устройствам, размещенным за NAT в удаленном офисе. Для решения этой проблемы вы можете включить в свойствах устройств, являющихся точками распространения, режим постоянного соединения с Сервером администрирования (флажок **Не разрывать соединение с Сервером администрирования**). Этот режим доступен, если общее количество точек распространения не превышает 300. Используйте push-серверы, чтобы обеспечить постоянную связь между управляемым устройством и Сервером администрирования. Дополнительную информацию см. в статье Включение push-сервера.

Выбор структуры защиты организации

Выбор структуры защиты организации определяют следующие факторы:

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

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

Для анализа сетевой и аппаратной инфраструктуры рекомендуется следующий порядок действий:

1. Определить следующие параметры сети, в которой будет развертываться защита:
   - число сегментов сети;
   - скорость каналов связи между отдельными сегментами сети;
   - число управляемых устройств в каждом из сегментов сети;
   - пропускную способность каждого канала связи, которая может быть выделена для работы защиты.
2. Определить допустимое время выполнения ключевых операций администрирования для всех управляемых устройств.
3. Проанализировать информацию из пунктов 1 и 2, а также данные нагрузочного тестирования системы администрирования. На основании проведенного анализа ответить на следующие вопросы:
   - Возможно ли обслуживание всех клиентов одним Сервером администрирования или требуется иерархия Серверов администрирования?
   - Какая аппаратная конфигурация Серверов администрирования требуется для обслуживания всех клиентов за время, определенное в пункте 2?
   - Требуется ли использование точек распространения для снижения нагрузки на каналы связи?

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

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

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

Типовые способы развертывания системы защиты

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

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

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

- Развертывание системы защиты с помощью Kaspersky Security Center Web Console.

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

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

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

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

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

Выбор СУБД

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

СУБД	Рекомендации и ограничения
MySQL (см. поддерживаемые версии)	Используйте эту СУБД, если вы планируете запустить один Сервер администрирования менее чем на 20 000 устройствах.
MariaDB (см. поддерживаемые версии)	Используйте эту СУБД, если вы планируете запустить один Сервер администрирования менее чем на 20 000 устройствах.
PostgreSQL, Postgres Pro (см. поддерживаемые версии)	Используйте эту СУБД, если вы планируете запустить один Сервер администрирования менее чем на 50 000 устройствах.
Tantor (см. поддерживаемые версии)	Используйте эту СУБД, если вы планируете запустить один Сервер администрирования менее чем на 50 000 устройствах. СУБД Tantor поддерживается только в Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8).

Подробнее о том как установить выбранную СУБД, см. в документации к этой СУБД.

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

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

Если вы установите 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.

Предоставление доступа к Серверу администрирования из интернета

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

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

По умолчанию Сервер администрирования не требует подключения к интернету для установки обновлений приложений Microsoft на управляемые устройства. Например, управляемые устройства могут загружать обновления приложений Microsoft непосредственно с серверов обновлений Microsoft или с Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации. Сервер администрирования должен быть подключен к интернету в следующих случаях:

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

- Закрытие уязвимостей в приложениях сторонних производителей

  Подключение Сервера администрирования к интернету необходимо для выполнения следующих задач:

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

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

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

Доступ из интернета: Сервер администрирования в локальной сети

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

Доступ из интернета: Сервер администрирования в демилитаризованной зоне

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

- Сервер администрирования не может самостоятельно обнаруживать новые устройства.
- Сервер администрирования не может выполнять первоначальное развертывание Агента администрирования посредством принудительной установки на устройства внутренней сети организации.

  Речь идет только о первоначальной установке Агента администрирования. Последующие обновления версии Агента администрирования или установка приложения безопасности уже могут быть выполнены Сервером администрирования.

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

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

Для успешной отправки уведомлений управляемым устройствам, размещенным во внутренней сети организации, на порт 15000 UDP, следует покрыть всю сеть предприятия точками распространения. В свойствах назначенных точек распространения установите флажок **Не разрывать соединение с Сервером администрирования**. В результате Сервер администрирования будет иметь постоянную связь с точками распространения, а точки распространения смогут посылать уведомления на порт 15000 UDP устройствам, размещенным во внутренней сети организации (это может быть IPv4-сеть или IPv6-сеть).

Установка

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

Настройка сервера MariaDB x64 для работы с Kaspersky Security Center Linux

Чтобы настроить сервер MariaDB x64 для работы с Kaspersky Security Center, необходимо использовать параметры сервера по умолчанию, если в этой статье не указаны иные параметры.

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=< 80% оперативной памяти, выделенной для СУБД; рекомендации см. в документации СУБД >
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
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

   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. Если вы используете MariaDB 10.4.3 или более раннюю версию, фактический размер выделенной памяти примерно на 10 процентов превышает указанный размер буфера. Рекомендации по настройке параметра `innodb_buffer_pool_size` и иную 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 MariaDB. Убедитесь, что для параметра `innodb_file_per_table` установлено значение `1`.

   Для MariaDB 10.1 дополнительно введите в раздел [mysqld] следующие строки:

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=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.

Вам нужно увеличить установленное по умолчанию максимальное количество файлов, которые можно открывать (файловые дескрипторы) для службы MariaDB systemd для обеспечения устойчивости под нагрузкой.

Чтобы увеличить максимальное количество файловых дескрипторов:

1. Выполните следующую команду:

   ```
   sudo systemctl edit mariadb.service
   ```

2. Укажите максимальное количество файловых дескрипторов в параметре `LimitNOFILE` в секции `[Service]`:

   ```
   LimitNOFILE=1048576
   ```

3. Выполните следующую команду, чтобы убедиться, что параметры указаны правильно:

   ```
   sudo systemd-analyze verify mariadb.service
   ```

4. Выполните следующую команду, чтобы перезагрузить процесс systemd:

   ```
   sudo systemctl daemon-reload
   ```

5. Выполните следующую команду, чтобы перезапустить службу MariaDB:

   ```
   sudo systemctl restart mariadb.service
   ```

   Максимальное количество файловых дескрипторов увеличено.

Настройка сервера СУБД на основе PostgreSQL для работы с Kaspersky Security Center Linux

В этой статье описана настройка Сервера администрирования, развернутого на одном устройстве. Если вы используете кластер высокой доступности СУБД, ознакомьтесь со статьей Подготовка кластера высокой доступности СУБД для работы с Kaspersky Security Center Linux.

Kaspersky Security Center Linux поддерживает СУБД на основе PostgreSQL. Чтобы настроить сервер СУБД на основе PostgreSQL для работы с Kaspersky Security Center Linux, необходимо использовать параметры сервера по умолчанию, если в этой статье не указаны иные параметры.

Путь по умолчанию к конфигурационному файлу:
`/etc/postgresql/<VERSION>/main/postgresql.conf`
В операционной системе Альт Linux по умолчанию используется путь
`/var/lib/pgsql/data/postgresql.conf`

Чтобы подготовить СУБД к установке Kaspersky Security Center Linux:

1. Настройте обязательные параметры сервера СУБД в соответствии с документацией соответствующей СУБД.

2. Для оптимизации работы СУБД с Kaspersky Security Center Linux укажите следующие параметры:

   - `max_connections = 151`
   - `shared_buffers = N`

     N = 25% от расчетного объема оперативной памяти для СУБД. Если СУБД установлена на устройстве, на котором также установлен Сервер администрирования, расчет следует производить на основе оперативной памяти, выделенной для СУБД, а не общей оперативной памяти устройства.

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

   Если вы используете Postgres Pro 15.7 или Postgres Pro 15.7.1, выключите параметр `enable_compound_index_stats`:

   `enable_compound_index_stats = off`

   После обновления конфигурационного файла примените конфигурацию или перезапустите службу СУБД командой:

   `sudo systemctl restart postgresql-<version>`

   или

   `sudo systemctl restart postgresql`

3. Создайте базы данных и учетные записи.

   Инструкцию по созданию баз и настройке учетных записей для СУБД на основе PostgreSQL см. в статье Создание баз и учетных записей СУБД на основе PostgreSQL.

СУБД готова к установке Kaspersky Security Center Linux.

Настройка сервера MySQL x64 для работы с Kaspersky Security Center Linux

Чтобы настроить сервер MySQL x64 для работы с Kaspersky Security Center, необходимо использовать параметры сервера по умолчанию, если в этой статье не указаны иные параметры.

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 секции `[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=<80% of the RAM allocated to the DBMS; see the DBMS
documentation for recommendations>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (in most cases, the server uses small transactions)
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. Рекомендации по настройке параметра `innodb_buffer_pool_size` и иную 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`.

Подготовка кластера высокой доступности СУБД для работы с Kaspersky Security Center Linux

В этой статье описаны действия по подготовке кластера высокой доступности СУБД для работы с Kaspersky Security Center Linux. Если Сервер администрирования развернут на одном устройстве, ознакомьтесь со статьей Настройка сервера СУБД на основе PostgreSQL для работы с Kaspersky Security Center Linux.

Kaspersky Security Center Linux поддерживает следующие кластеры высокой доступности:

- Platform V Pangolin.
- Postgres Pro Built-in High Availability.
- Patroni (с опциональным балансировщиком нагрузки HAProxy).

Минимальная рекомендуемая конфигурация кластера высокой доступности СУБД должна включать не менее трех узлов.

Чтобы подготовить кластер высокой доступности СУБД для работы с Kaspersky Security Center Linux:

1. Установите тип репликации синхронным.

   Если вы используете шаблон Patroni версии 3.3.1 или ниже для PostgreSQL, убедитесь, что параметр `synchronous_standby_names` применен правильно.

   Чтобы проверить используется ли синхронная репликация, выполните следующий запрос на управляющем узле:

   `SELECT application_name, client_addr, client_hostname, client_port, sync_state FROM pg_stat_replication;`

   Если в столбце `sync_state` любого узла отображаются значения, отличные от `sync` или `potential`, кластер использует асинхронную репликацию, которая не поддерживается. Чтобы решить эту проблему, выполните одно из следующих действий:

   Обновите Patroni до версии 3.3.2 или выше.

   В конфигурационном файле Patroni найдите подсекцию `dcs` секции `bootstrap` и установите для параметра `synchronous_mode` значение `true`:

   ```
   bootstrap:
   dcs:
   <...>
   synchronous_mode: true
   ```

2. На каждом узле кластера СУБД настройте конфигурационный файл, выполнив шаги 1 и 2 инструкции Настройка сервера СУБД на основе PostgreSQL для работы с Kaspersky Security Center Linux.

3. Создайте базы данных и учетные записи по инструкции в статье Создание баз и учетных записей СУБД на основе PostgreSQL.

4. Настройте обнаружение узлов кластера СУБД одним из следующих способов:

   - Вручную укажите все узлы кластера СУБД в процессе установки Kaspersky Security Center Linux.
   - Для автоматического обнаружения узлов кластера укажите только DNS-имя или IP-адрес управляющего узла или узла-реплики в процессе установки Kaspersky Security Center Linux.

     Для этого выполните следующие действия:

     a. На всех узлах кластера высокой доступности СУБД добавьте следующую строку в конфигурационный файл `postgresql`:

     `log_hostname=1`

     b. После изменения конфигурационного файла перезагрузите службу кластера СУБД на всех узлах кластера СУБД высокой доступности.

     c. Убедитесь, что у пользователя базы данных есть привилегия `pg_read_all_stats`.

     Вы можете предоставить эту привилегию, выполнив следующую команду:

     `GRANT pg_read_all_stats TO "<kscdbadmin>";`

     Где `<kscdbadmin>` – имя пользователя базы данных.

     Имя пользователя базы данных Сервера администрирования указывается при установке Kaspersky Security Center Linux.

     d. Настройте балансировщик нагрузки для базы данных IAM.

Кластер высокой доступности СУБД готов к работе с Kaspersky Security Center Linux.

Установка Kaspersky Security Center Linux

В этом разделе описана установка Kaspersky Security Center Linux.

Перед установкой приложения выполните следующие действия:

- Спроектируйте развертывание Kaspersky Security Center Linux в соответствии с рекомендациями сценария Начало работы.

  Если вы выполнили предварительные требования и шаги 1-4 сценария, приступайте к установке Сервера администрирования Kaspersky Security Center Linux.

  > Если вы используете операционную систему РЕД ОС 7.3.4 и выше или МСВСфера 9.2 и выше, установите пакет libxcrypt-compat для корректной работы Сервера администрирования.

- Установите СУБД для Kaspersky Security Center Linux. Вы можете выбрать одну из поддерживаемых СУБД.

  Если дистрибутив вашей операционной системы на базе Linux не содержит поддерживаемую СУБД, вы можете установить СУБД из стороннего официального репозитория разработчика или другого доверенного источника.

После установки СУБД выполните соответствующую инструкцию:

- Настройка сервера СУБД на основе PostgreSQL для работы с Kaspersky Security Center Linux
- Настройка сервера MariaDB x64 для работы с Kaspersky Security Center Linux
- Настройка сервера MySQL x64 для работы с Kaspersky Security Center Linux

- Убедитесь, что DNS-сервер доступен в сети.

  FQDN-адреса и DNS-имена серверных компонентов Kaspersky Security Center Linux должны успешно преобразовываться в IP-адреса в операционных системах компонентов приложения и на устройствах сети.

- Загрузите установочный файл нужной локализации с сайта "Лаборатории Касперского".

  Выберите установочный файл, соответствующий дистрибутиву Linux, установленному на вашем устройстве, ksc64_<номер_версии>_amd64.deb или ksc64-<номер_версии>.x86_64.rpm.

  > Язык установленного Сервера администрирования зависит от локализации загруженного дистрибутива.

Чтобы установить Kaspersky Security Center Linux:

1. Создайте группу безопасности для служб Kaspersky Security Center, непривилегированную учетную запись для запуска служб Сервера администрирования, непривилегированную учетную запись для запуска служб IAM.

   Учетные записи должны быть членами группы безопасности Kaspersky Security Center.

   Для этого последовательно выполните следующие команды (в этом примере: группа безопасности – "kladmins", учетная запись для запуска служб Сервера администрирования – "ksc", учетная запись для запуска служб IAM – "ksciam"):

   ```
   sudo adduser ksc
   sudo groupadd kladmins
   sudo gpasswd -a ksc kladmins
   sudo usermod -g kladmins ksc
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

2. При необходимости увеличьте установленное по умолчанию максимальное количество файлов, которые можно открывать (файловые дескрипторы) для учетных записей, используемых для работы служб Сервера администрирования.

   Для этого откройте файл /etc/security/limits.conf и укажите мягкие и жесткие ограничения файловых дескрипторов следующим образом:

   ```
   ksc soft nofile <max_number_of_opened_files>
   ksc hard nofile <max_number_of_opened_files>
   ```

   По умолчанию ограничения дескрипторов файлов указываются во время установки. Мягкие ограничения файлов составляют 32 768 файлов, жесткие ограничения файлов составляют 131 072 файла.

3. Запустите установку Kaspersky Security Center Linux.

   В зависимости от вашего дистрибутива Linux выполните одну из следующих команд:

`sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb`

`sudo yum install /<path>/ksc64-<version_number>.x86_64.rpm`

4. Запустите скрипт первоначальной настройки Kaspersky Security Center Linux:

   `/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 Linux, вам нужно 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) в соответствии с Политикой конфиденциальности. Введите `n`, если вы не принимаете условия Политики конфиденциальности. Чтобы использовать Kaspersky Security Center Linux, вам нужно принять условия Политики конфиденциальности.

6. При отображении запроса введите следующие параметры:

   a. Выберите значение **Стандартный**, в качестве режима установки Сервера администрирования.

   b. Введите FQDN или DNS-имя Сервера администрирования. Имя будет использоваться другими устройствами для подключения к Серверу администрирования.

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

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

      - Если число управляемых устройств составляет от 1 до 100, введите 1.
      - Если число управляемых устройств составляет от 101 до 1000, введите 2.
      - Если число управляемых устройств составляет более 1000, введите 3.

      Этот параметр используется для автоматического определения случайной задержки запуска задач в целях оптимизации нагрузки на сеть. В списке ниже показан интервал, в пределах которого рассчитывается эта задержка:

      - От 1 до 100 управляемых устройств, значение 1. Без задержки.
      - От 101 до 1000 управляемых устройств, значение 2. Задержка 5 минут.
      - Более 1000 управляемых устройств, значение 3. Задержка 10 минут.

   e. Введите имя группы безопасности, созданной на шаге 1 (в примере группа `kladmins`).

   f. Введите имя учетной записи для запуска службы Сервера администрирования, созданной на шаге 1 (в примере учетная запись `ksc`).

      Учетная запись должна быть членом группы безопасности, которую вы указали на шаге 8e.

g. Введите имя учетной записи, чтобы запустить другие службы (в примере группа `kladmins`).

Учетная запись должна быть членом группы безопасности, которую вы указали на шаге 8e.

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

- Если вы установили MySQL или MariaDB, введите 1.
- Если вы установили СУБД на основе PostgreSQL, введите 2.

i. Введите DNS-имя или IP-адрес устройства, на котором установлена СУБД Сервера администрирования. Адрес для локальной установки СУБД – 127.0.0.1.

Чтобы использовать отказоустойчивый кластер высокой доступности, выполните одно из следующих действий:

- Введите DNS-имена или IP-адреса и порты всех узлов в следующем формате:
  `<fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;`
- Укажите только DNS-имя или IP-адрес управляющего узла или узла-реплики.

j. Введите номер порта базы данных. Этот порт используется для связи с Сервером администрирования. Пропустите этот шаг, если на шаге 8i вы ввели DNS-имена или IP-адреса и порты всех узлов кластера высокой доступности.

По умолчанию используются следующие порты:

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

k. Введите имя базы данных Сервера администрирования (в примере в статьях база данных `kav`), которую вы создали по инструкции Создание баз и учетных записей СУБД на основе PostgreSQL либо Настройка сервера MariaDB x64 для работы с Kaspersky Security Center Linux.

l. Введите имя учетной записи администратора базы данных, которая используется для доступа к базе данных Сервера администрирования (в примере в статьях из пункта 8k `kscdbadmin`).

m. Введите пароль учетной записи администратора базы данных, которая используется для доступа к базе данных Сервера администрирования.

n. Если вы установили СУБД на основе PostgreSQL, вы можете указать схему базы данных, которая будет использоваться Сервером администрирования. Для этого укажите имя схемы.

> Имя схемы чувствительно к регистру. Используйте только строчные буквы.

Если вы не хотите использовать пользовательскую схему, нажмите ENTER. В этом случае будет использоваться схема, выбранная в СУБД в качестве схемы по умолчанию.

o. Введите FQDN или DNS-имя сервера IAM. Если вы не укажете эту переменную, будет использовано DNS-имя устройства, на котором установлен Сервер администрирования.

Укажите значение, которое вы указали на шаге 8b.

p. Введите имя учетной записи для запуска службы IAM, созданной на шаге 1. Учетная запись должна быть членом указанной группы безопасности, которую вы указали на шаге 8e (в примере на шаге 1 `ksciam`).

q. Выберите СУБД, которую вы установили для работы со службой IAM:

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

r. Введите адрес СУБД IAM, который будет использоваться службой IAM.

Чтобы использовать кластер высокой доступности, выполните одно из следующих действий:

- Введите DNS-имена или IP-адреса и порты всех узлов в следующем формате:
  `<fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;`
- Укажите только DNS-имя или IP-адрес балансировщика нагрузки.

s. Введите номер порта СУБД IAM. Этот порт используется для связи со службой IAM. Пропустите этот шаг, если на шаге 8r вы ввели DNS-имена или IP-адреса и порты всех узлов кластера высокой доступности.

По умолчанию используются следующие порты:

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

t. Введите имя базы данных IAM, которое будет использоваться службой IAM (в примере `iam`).

u. Введите имя учетной записи администратора базы данных, которая используется для доступа к базе данных IAM (в примере `iamdbadmin`).

v. Введите пароль учетной записи администратора базы данных, которая используется для доступа к базе данных IAM.

Подождите, пока службы добавятся и запустятся автоматически:

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

w. Если вы установили PostgreSQL или Postgres Pro, вы можете указать схему базы данных, которая будет использоваться IAM. Для этого укажите имя схемы.

Если вы не хотите использовать пользовательскую схему, нажмите ENTER. В этом случае будет использоваться схема public.

> Имя схемы чувствительно к регистру. Используйте только строчные буквы.
> Не указывайте зарезервированные имена схем IAM: client, iam, ksc, locker, pat, scope, voltron.

x. 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 256 символов.
- Пароль должен содержать символы как минимум трех групп из списка ниже:
  - верхний регистр (A–Z);
  - нижний регистр (a–z);
  - числа (0–9);
  - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).

Если пропустить этот шаг, позже вы сможете воспользоваться следующей командой для создания пользователя:

```
/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p
```

Пользователь добавлен, и Kaspersky Security Center Linux установлен.

Переходите к установке Kaspersky Security Center Web Console.

Если у Сервера Администрирования нет доступа к хранилищу дистрибутивов приложений для удаленной установки, то для загрузки зависимостей, необходимых, чтобы создать инсталляционные пакеты для установки приложений на устройства Windows, выполните следующие действия:

1. Создайте флаг RIUtilsArchiveDirUsed с помощью команды:

   `/opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1`

2. Скачайте дополнительные модули Files for remote installation via Kaspersky Security Center с сайта "Лаборатории Касперского".

   Скачанные архивы имеют следующие имена:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Не переименовывайте архивы.

3. Поместите архивы в директорию /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

4. Перезапустите службу Сервера администрирования с помощью команды:

   `systemctl restart kladminserver_srv.service`

Теперь у Сервера администрирования есть нужные зависимости.

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`
- `systemctl status kliam_srv.service`

Установка Kaspersky Security Center Linux 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 СУБД для Kaspersky Security Center Linux. Вы можете выбрать одну из поддерживаемых СУБД. Подробнее о том как установить выбранную СУБД, см. в документации к этой СУБД.

  Если дистрибутив вашей операционной системы на базе Linux не содержит поддерживаемую СУБД, вы можете установить СУБД из стороннего хранилища пакетов.

  После установки СУБД выполните соответствующую инструкцию:

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

    Настройка учетной записи СУБД для работы с PostgreSQL и Postgres Pro

    Если вы хотите, чтобы Сервер администрирования автоматически обнаруживал адреса узлов кластера, вам нужно указать только DNS-имя или IP-адрес управляющего узла или узла-реплики во время установки. Для этого убедитесь, что вы выполнили шаг 2 инструкции Подготовка кластера высокой доступности СУБД для работы с Kaspersky Security Center Linux.

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

    Настройка учетной записи СУБД для работы с MySQL и MariaDB

  - Настройка сервера MySQL x64 для работы с Kaspersky Security Center Linux

    Настройка учетной записи СУБД для работы с MySQL и MariaDB

- Убедитесь, что на вашем устройстве с установленной СУБД нет учетных записей пользователей СУБД со следующими именами:
  - client
  - iam
  - ksc

- locker
- pat
- scope
- voltron

- Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center Linux, работает один из поддерживаемых дистрибутивов Linux.

  Если вы используете операционную систему РЕД ОС 7.3.4 и выше или МСВСфера 9.2 и выше, установите пакет libxcrypt-compat для корректной работы Сервера администрирования.

- Загрузите установочный файл нужной локализации с сайта "Лаборатории Касперского". Выберите установочный файл, соответствующий дистрибутиву Linux, установленному на вашем устройстве, ksc64_[version_number]_amd64.deb или ksc64-[version_number].x86_64.rpm.

Чтобы установить Kaspersky Security Center Linux в тихом режиме:

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

2. Создайте группу kladmins и непривилегированные учетные записи ksc и ksciam, которые должны быть членами 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`

   `adduser ksciam`

   `gpasswd -a ksciam kladmins`

   `usermod -g kladmins ksciam`

3. На сервере СУБД создайте базу данных для IAM. Имя базы данных должно отличаться от имени базы данных, которую вы установили для работы с Kaspersky Security Center Linux. Сервер администрирования не удаляет базу данных IAM автоматически при деинсталляции или переносе Сервера на другое устройство, вам нужно удалить базу данных вручную.

   - Для PostgreSQL выполните команду:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - Для MariaDB выполните команду:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

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 для переменной среды `KLAUTOANSWERS` в среде root или пользователя значение, содержащее полное имя файла ответов, включая путь, например, с помощью следующей команды:

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

6. Запустите установку Kaspersky Security Center Linux в тихом режиме и в зависимости от вашего дистрибутива Linux выполните одну из следующих команд:

   В корневой среде:

```
apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

```
yum install /<path>/ksc64-[version_number].x86_64.rpm -y
```

   В пользовательской среде:

```
sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

```
sudo -E yum install /<path>/ksc64-[version_number].x86_64.rpm -y
```

7. Создайте учетную запись для работы с Kaspersky Security Center Web Console. Для этого выполните следующую команду под учетной записью с правами root и укажите пароль длиной минимум 8 символов:

```
/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>
```

8. Установите Kaspersky Security Center Web Console.

Переменные файла ответов, используемые в качестве параметров установки Kaspersky Security Center Linux 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 порта для работы с OpenAPI. Также этот порт используется для входящих подключений от Kaspersky Security Center Web Console. Необязательный параметр. По умолчанию указано значение 13299.	Номер порта

KLSRV_UNATT_PORT_GUI	Нет	Номер порта для работы с утилитой klakaut. Необязательный параметр. По умолчанию указано значение 13291. Утилита klakaut и справочная система для нее расположены в папке установки Kaspersky Security Center Linux. По умолчанию порт закрыт. Если вы хотите использовать утилиту klakaut для автоматизации работы Kaspersky Security Center Linux, откройте порт 13291 с помощью утилиты klscflag.	Номер порта
KLSRV_UNATT_NETRANGETYPE	Нет	Примерное количество устройств, которыми вы планируете управлять. Этот параметр используется для оптимизации нагрузки на сеть. Необязательный параметр. По умолчанию указано значение 1.	1 от 1 до 100 управляемых устройств. 2 от 101 до 1000 управляемых устройств. 3 более 1000 управляемых устройств.
KLSRV_UNATT_DBMS_TYPE	Да	Тип системы управления базой данных: MySQL (MariaDB) или Postgres.	mysql или postgres
KLSRV_UNATT_DBMS_INSTANCE	Да	Адрес сервера базы данных. Чтобы использовать PostgreSQL, кластер Postgres Pro Built-in High Availability или кластер СУБД Platform V Pangolin, введите DNS-имена или IP-адреса и порты всех узлов в следующем формате: <fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>; Если вы хотите использовать кластер СУБД Platform V Pangolin, вы можете указать только DNS-имя или IP-адрес управляющего узла или реплики узла при указании адреса СУБД.	DNS-имя или статический IP-адрес сервера базы данных.
KLSRV_UNATT_DBMS_PORT	Да	Порт сервера базы данных. Значение по умолчанию для MySQL (MariaDB) – 3306; для Postgres – 5432.	3306 или 5432
KLSRV_UNATT_DB_NAME	Да	Имя базы данных. Имя базы данных должно отличаться от имени базы данных IAM, указанного в переменной KLSRV_UNATT_DB_IAM_NAME.	kav
KLSRV_UNATT_DBMS_LOGIN	Да	Имя пользователя, который имеет доступ к базе данных.	
KLSRV_UNATT_DBMS_PASSWORD	Да	Пароль пользователя, который имеет доступ к базе данных.	
KLSRV_UNATT_DBMS_SCHEMA	Нет	Пользовательская схема СУБД. Если вы не укажете пользовательскую схему, Сервер администрирования будет использовать схему по умолчанию. Имя схемы чувствительно к регистру. Используйте только строчные буквы. Вы можете указать пользовательскую схему только в том случае, если PostgreSQL или Postgres Pro используются в качестве СУБД. Иначе переменная игнорируется.	database_schema

KLSRV_UNATT_IAM_ADDRESS	Да	Пользовательские браузеры будут перенаправлены на этот адрес с помощью OpenID Connect. Введите FQDN сервера IAM. Вам нужно использовать DNS-имя Сервера администрирования, указанное в параметре KLSRV_UNATT_SERVERADDRESS.	FQDN
KLSRV_UNATT_KLIAMUSER	Да	Имя учетной записи для запуска службы IAM. Учетная запись должна быть членом группы безопасности, указанной в переменной KLSRV_UNATT_KLADMINSGROUP.	ksciam
KLSRV_UNATT_DBMS_IAM_TYPE	Да	Тип системы управления базой данных IAM: MySQL (MariaDB) или Postgres.	mysql Или postgres
KLSRV_UNATT_DBMS_IAM_INSTANCE	Да	Адрес сервера базы данных IAM. Чтобы использовать PostgreSQL, кластер Postgres Pro Built-in High Availability или кластер СУБД Platform V Pangolin, введите DNS-имена или IP-адреса и порты всех узлов в следующем формате: <fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>; Если вы хотите использовать кластер СУБД Platform V Pangolin, вы можете указать только DNS-имя или IP-адрес управляющего узла или реплики узла при указании адреса СУБД.	IP-адрес;
KLSRV_UNATT_DBMS_IAM_PORT	Да	Порт сервера базы данных IAM. Значение по умолчанию для MySQL (MariaDB) – 3306; для Postgres – 5432.	3306 Или 5432
KLSRV_UNATT_DBMS_IAM_LOGIN	Да	Имя пользователя, имеющего доступ к базе данных IAM. Если типом базы данных IAM является MySQL (MariaDB) и есть оба следующих параметра: • gtid_mode=ON • gtid_purged=ON|AUTO Убедитесь, что указанный пользователь имеет одну из следующих привилегий СУБД: • RELOAD • FLUSH_TABLES	
KLSRV_UNATT_DBMS_IAM_PASSWORD	Да	Пароль пользователя, который имеет доступ к базе данных IAM.	

KLSRV_UNATT_DBMS_IAM_SCHEMA	Нет	Пользовательская схема СУБД. Если вы не укажете пользовательскую схему, IAM будет использовать общедоступную схему. Вы можете указать пользовательскую схему только в том случае, если PostgreSQL или Postgres Pro используются в качестве СУБД. Иначе переменная игнорируется. Имя схемы чувствительно к регистру. Используйте только строчные буквы. Не указывайте зарезервированные имена схем IAM: client, iam, ksc, locker, pat, scope, voltron.	database_schema
KLSRV_UNATT_DB_IAM_NAME	Да	Имя базы данных IAM. Имя базы данных IAM должно отличаться от имени базы данных, указанного в переменной KLSRV_UNATT_DB_NAME. Укажите пустую базу данных, созданную вручную.	iamdb
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 Linux, файл ответов должен включать следующие дополнительные переменные:			
KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT	Нет	Конфигурация отказоустойчивого кластера. Если параметр не указан в файле ответов, используется значение по умолчанию. Возможные значения: 0 – отказоустойчивый кластер, узлы которого расположены в едином центре обработки данных (значение по умолчанию); 2 – геораспределенный отказоустойчивый кластер, узлы которого расположены в разных центрах обработки данных.	0 или 2
KLFOC_UNATT_NODE	Да	Номер узла (1 или 2).	1 или 2
KLFOC_UNATT_STATE_SHARE_MOUNT_PATH	Да	Точка монтирования общей папки состояния.	
KLFOC_UNATT_DATA_SHARE_MOUNT_PATH	Да	Точка монтирования 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

Если у Сервера Администрирования нет доступа к хранилищу дистрибутивов приложений для удаленной установки, то для загрузки зависимостей, необходимых, чтобы создать инсталляционные пакеты для установки приложений на устройства Windows, выполните следующие действия:

1. Создайте флаг RIUtilsArchiveDirUsed с помощью команды:

   `/opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1`

2. Скачайте дополнительные модули Files for remote installation via Kaspersky Security Center с сайта "Лаборатории Касперского".

   Скачанные архивы имеют следующие имена:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Не переименовывайте архивы.

3. Поместите архивы в директорию /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

4. Перезапустите службу Сервера администрирования с помощью команды:

   `systemctl restart kladminserver_srv.service`

Теперь у Сервера администрирования есть нужные зависимости.

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

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

Перед установкой:

- Установите СУБД.
- Загрузите ключ приложения kaspersky_astra_pub_key.gpg.
- Загрузите установочный файл ksc64_[номер_версии]_amd64.deb с сайта "Лаборатории Касперского".

Под учетной записью с привилегиями root выполняйте команды, представленные в этой инструкции, с высокой степенью целостности и нулевой конфиденциальности.

Чтобы установить Kaspersky Security Center Linux на устройство с операционной системой Astra Linux Special Edition (очередное обновление 1.7.2), Astra Linux Special Edition (очередное обновление 1.6) и Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8):

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

   ```
   DIGSIG_ELF_MODE=1
   ```

2. В командной строке введите следующую команду, чтобы установить пакет совместимости:

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

3. Создайте директорию для ключа приложения:

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

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

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

5. Обновите исходный образ файловой системы RAM для всех ядер системы:

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

   Перезагрузите систему.

6. Создайте группу "kladmins" и непривилегированные учетные записи "ksc" и "ksciam". Учетные записи должны быть членами группы "kladmins". Для этого последовательно выполните следующие команды:

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

7. Запустите установку Kaspersky Security Center Linux:

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

8. Запустите настройку Kaspersky Security Center Linux:

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

9. 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 Linux, вам нужно 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) в соответствии с Политикой конфиденциальности. Введите `n`, если вы не принимаете условия Политики конфиденциальности. Чтобы использовать Kaspersky Security Center Linux, вам нужно принять условия Политики конфиденциальности.

10. При отображении запроса введите следующие параметры:

    a. Введите FQDN или DNS-имя Сервера администрирования.

    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 число управляемых устройств составляет от 1 до 100, введите 1.
    - Если число управляемых устройств составляет от 101 до 1000, введите 2.
    - Если число управляемых устройств составляет более 1000, введите 3.

    Этот параметр используется для автоматического определения случайной задержки запуска задач в целях оптимизации нагрузки на сеть. В списке ниже показан интервал, в пределах которого рассчитывается эта задержка:

    - От 1 до 100 управляемых устройств, значение 1. Без задержки.
    - От 101 до 1000 управляемых устройств, значение 2. Задержка 5 минут.
    - Более 1000 управляемых устройств, значение 3. Задержка 10 минут.

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

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

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

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

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

    k. Введите имя базы данных.

    l. Введите имя учетной записи администратора базы данных, которая используется для доступа к базе данных.

    m. Введите пароль учетной записи администратора базы данных, которая используется для доступа к базе данных.

n. Введите FQDN или DNS-имя сервера IAM.

Укажите значение, которое вы указали на шаге 10a.

o. Введите имя учетной записи для запуска службы kliam. Учетная запись должна быть членом указанной группы безопасности.

p. Выберите СУБД, которую вы установили для работы со службой IAM:

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

q. Введите адрес СУБД, который будет использоваться службой IAM.

r. Введите номер порта базы данных. Этот порт используется для связи со службой IAM. По умолчанию используются следующие порты:

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

s. Введите имя базы данных, которое будет использоваться службой IAM. Имя базы данных, используемой службой IAM, должно отличаться от имени базы данных, используемой Сервером администрирования.

t. Введите имя корневой учетной записи базы данных, которая используется для доступа к базе данных IAM.

u. Введите пароль корневой учетной записи базы данных, которая используется для доступа к базе данных IAM.

Подождите, пока службы добавятся и запустятся автоматически:

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

v. Создайте учетную запись, которая будет выполнять роль администратора Сервера администрирования. Введите имя пользователя и пароль.

Пароль должен соответствовать следующим правилам:

- Пароль пользователя должен содержать не менее 8 символов, но не более 256.
- Пароль должен содержать символы как минимум трех групп из списка ниже:
  - верхний регистр (A–Z);
  - нижний регистр (a–z);

- числа (0–9);
- специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).

Приложение Kaspersky Security Center Linux установлено и пользователь добавлен.

Для загрузки зависимостей, необходимых, чтобы создать инсталляционные пакеты для установки приложений на устройства Windows, выполните следующие действия:

1. Создайте флаг RIUtilsArchiveDirUsed с помощью команды:

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Скачайте дополнительные модули Files for remote installation via Kaspersky Security Center с сайта "Лаборатории Касперского".

   Скачанные архивы имеют следующие имена:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Не переименовывайте архивы.

3. Поместите архивы в директорию /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

4. Перезапустите службу Сервера администрирования с помощью команды:

   ```
   systemctl restart kladminserver_srv.service
   ```

Теперь у Сервера администрирования есть нужные зависимости.

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`
- `# systemctl status kliam_srv.service`

Установка Kaspersky Security Center Web Console

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

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

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.

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

Чтобы установить Kaspersky Security Center Web Console:

1. Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center Web Console, работает один из поддерживаемых дистрибутивов Linux.
2. Прочитайте Лицензионное соглашение. Если в состав дистрибутива Kaspersky Security Center Linux 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 приложение.
3. Создайте файл ответов, который содержит параметры для подключения Kaspersky Security Center Web Console к Серверу администрирования: `/etc/ksc-web-console-setup.json`.

   Пример файла ответов с минимальным набором параметров

   Набор параметров файла ответов зависит от версии Сервера администрирования, к которому подключено приложение Kaspersky Security Center Web Console:

   - Сервер администрирования версии 16 и выше

     Пример файла ответов с минимальным набором параметров для входа на Сервер администрирования версии 16 и выше:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Сервер администрирования версии 15.4 и выше

  Пример файла ответов с минимальным набором параметров для входа на Сервер администрирования версии 15.4 и ниже:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Вы можете установить Kaspersky Security Center Web Console на том же устройстве, что и Сервер администрирования, или на другом устройстве. Если приложение Kaspersky Security Center Web Console установлено на другом устройстве, адрес Kaspersky Security Center Web Console (параметр `address`) и адрес Сервера администрирования (параметр `iamHost` или `kscHost`) отличаются. Если приложение Kaspersky Security Center Web Console установлено на одном устройстве с Сервером администрирования, эти параметры имеют одинаковые значения.

Значение `iamHost` должно совпадать с адресом IAM, который вы указали при установке Сервера администрирования. Для получения указанного адреса IAM выполните следующую команду на устройстве с установленным Сервером администрирования:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Подробную информацию см. в статье Параметры установки Kaspersky Security Center Web Console.

Вы можете добавить несколько Серверов администрирования разных версий в список доверенных серверов. В этом случае Серверы могут использовать разные способы аутентификации.

Рекомендуется указывать номера портов больше 1024. Если вы хотите, чтобы приложение Kaspersky Security Center Web Console работало на портах ниже 1024, после установки убедитесь, что у вас установлена утилита setcap, а затем выполните команду:

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

Если у вас нет утилиты setcap, вы можете ее установить. **Перейдите по этой ссылке, чтобы просмотреть команды**

Для операционных систем Debian и Ubuntu выполните одну из следующих команд:

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

Для SUSE Linux Enterprise Server и Red Hat Enterprise Linux выполните команду:

- `sudo zypper install libcap-progs`

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

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

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

   - Чтобы установить или обновить предыдущую версию Kaspersky Security Center Web Console из файла .deb, выполните следующую команду:
     ```
     sudo apt-get install ksc-web-console-<build number>.x86_64.deb
     ```
   - Чтобы установить Kaspersky Security Center Web Console из файла .rpm, выполните одну из следующих команд:
     ```
     sudo yum install ksc-web-console-<build number>.x86_64.rpm
     ```
     Или
     ```
     sudo alien -i ksc-web-console-<build number>.x86_64.rpm
     ```
   - Чтобы обновить предыдущую версию Kaspersky Security Center Web Console, выполните одну из следующих команд:
     - Для устройств с операционными системами на базе RPM:
       ```
       sudo yum install ksc-web-console-<build number>.x86_64.rpm
       ```
     - Для устройств с операционными системами на базе Debian:
       ```
       sudo apt-get install ksc-web-console-<build number>.x86_64.deb
       ```

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

5. Перезапустите все службы Kaspersky Security Center Web Console, выполнив следующую команду:
   ```
   sudo systemctl restart KSC*
   ```

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

Если общий сертификат Сервера администрирования заменяется другим сертификатом из резервной копии или с помощью утилиты klsetsrvcert, вам нужно удалить, а затем переустановить Kaspersky Security Center Web Console. Иначе вход в Web Console будет ограничен.
Если после переустановки вы не можете войти в Web Console, проверьте конфигурацию сервера IAM.

Параметры установки Kaspersky Security Center Web Console

Для установки Сервера Kaspersky Security Center Web Console на устройства с операционными системами Linux необходимо создать файл ответов (файл .json), который содержит параметры подключения Kaspersky Security Center Web Console к Серверу администрирования. Вам нужно назвать этот файл ksc-web-console-setup.json и расположить его в директории /etc/ksc-web-console-setup.json.

Сервер администрирования включает в себя компонент Identity and Access Manager (IAM), который обеспечивает доменную аутентификацию с единым входом (SSO) в Kaspersky Security Center Web Console. Для подключения Kaspersky Security Center Web Console к Серверу администрирования файл ответов должен содержать параметры взаимодействия с IAM-компонентом, даже если вы не используете единый вход (SSO).

Пример файла ответов для установки приложения Web Console, которое будет подключаться к Серверу администрирования версии 16 и выше. В этом примере Web Console и Сервер администрирования установлены на разных устройствах:

```
{
    "webConsoleAddress": "ksc-web-console.example.com",
    "port": 8080,
    "defaultLangId": 1049,
    "enableLog": true,
    "trusted":  {
        "Administration Server v16": {
                "iamHost": "ksc16.example.com",
                "iamOAuthPort": 4444,
                "iamProxyPort": 9050,
                "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
                "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
                "kscPort": 13299,
                "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "acceptEula": true,
    "certPath": "/root/server.crt",
    "keyPath": "/root/key-without-passphrase.pem",
    "internalCertsTTLDays": 1095,
    "webConsoleAccount": "Group1:User1",
    "managementServiceAccount": "Group1:User2",
    "serviceWebConsoleAccount": "Group1:User3",
    "pluginAccount": "Group1:User4",
    "natsMessageQueueAccount": "Group1:User6"
}
```

Параметры `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount`, `natsMessageQueueAccount`, `certPath` и `keyPath` необязательные. Вы можете не указывать эти параметры в файле ответов.

Если вы хотите использовать пользовательский сертификат, укажите параметры `certPath` и `keyPath`. Если вы не укажете параметры или укажете только один, веб-браузер будет сообщать вам, что ваше подключение не защищено.

Из соображений безопасности не рекомендуется указывать параметры `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` и `natsMessageQueueAccount`.
Если вы решили указать эти параметры, убедитесь, что настраиваемые учетные записи пользователей принадлежат к одной и той же группе безопасности. Если эти параметры не указаны, установщик Kaspersky Security Center Web Console создает группу безопасности по умолчанию, а затем создает в этой группе учетные записи пользователей с именами по умолчанию.
Параметры `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` и `natsMessageQueueAccount` невозможно использовать отдельно друг от друга: укажите значения либо для всех этих параметров, либо ни для одного.

Вы можете установить Kaspersky Security Center Web Console на том же устройстве, что и Сервер администрирования, или на другом устройстве. Если приложение Kaspersky Security Center Web Console установлено на другом устройстве, адрес Kaspersky Security Center Web Console (параметр `webConsoleAddress`) и адрес Сервера администрирования (параметр `iamHost` или `kscHost`) отличаются. Если приложение Kaspersky Security Center Web Console установлено на одном устройстве с Сервером администрирования, эти параметры имеют одинаковые значения.

Значение `iamHost` должно совпадать с адресом IAM, указанным при установке Сервера администрирования. Для получения указанного адреса IAM выполните следующую команду на устройстве с установленным Сервером администрирования:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Рекомендуется указывать номера портов больше 1024. Если вы хотите, чтобы приложение Kaspersky Security Center Web Console работало 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
```

Если у вас нет утилиты setcap, вы можете ее установить. **Перейдите по этой ссылке, чтобы просмотреть команды**.

Для операционных систем Debian и Ubuntu выполните одну из следующих команд:

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

Для SUSE Linux Enterprise Server и Red Hat Enterprise Linux выполните команду:

- `sudo zypper install libcap-progs`

При установке Kaspersky Security Center Web Console на устройство с операционной системой Альт 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 Web Console на устройствах с операционными системами Linux

Параметр	Описание	Доступные значения
`webConsoleAddress`	Адрес устройства (FQDN или имя устройства), на котором установлено приложение Kaspersky Security Center Web Console (обязательный параметр). Если вы устанавливаете Kaspersky Security Center Web Console на Сервер Kaspersky Security Center, используйте адрес, который вы указали при установке Kaspersky Security Center Linux. Если вы устанавливаете Kaspersky Security Center Web Console на другое устройство, укажите адрес устройства (FQDN или имя устройства), который будет использоваться браузером для подключения к Серверу Kaspersky Security Center Web Console.	Строковое значение. Например: `"ksc.example.com"`
`port`	Порт, используемый Kaspersky Security Center Web Console для приема подключений от веб-браузеров (обязательный).	Числовое значение. Рекомендуемое значение – 8080 (за ис операционной системы Альт Linux).

Параметр	Описание	Доступные значения
`defaultLangId`	Язык пользовательского интерфейса (по умолчанию `1033`). При необходимости вы можете сменить язык интерфейса Kaspersky Security Center Web Console.	Числовой код языка: • Немецкий: `1031` • Английский: `1033` • Испанский: `1034` • Испанский (Мексика): `2058` • Французский: `1036` • Итальянский: `1040` • Японский: `1041` • Казахский: `1087` • Польский: `1045` • Португальский (Бразилия): `1046` • Русский: `1049` • Турецкий: `1055` • Упрощенный китайский: `2052` • Традиционный китайский: `1028` Если значение не указано, используетс язык (en-US).
`enableLog`	Включение или выключение журнала трассировки Kaspersky Security Center Web Console. Рекомендуется изменять значение параметра по умолчанию только по запросу специалиста Службы технической поддержки "Лаборатории Касперского".	Логическое значение: • `true` – ведение журнала включено • `false` – ведение журнала выключе по умолчанию).

Параметр	Описание	Доступные значения
`trusted`	Список адресов доверенных Серверов администрирования, к которым может подключаться Kaspersky Security Center Web Console. Вы можете добавить несколько Серверов администрирования разных версий в список доверенных серверов. Для Сервера администрирования версии 16 и выше: • имя Сервера администрирования, которое будет отображаться в окне входа. • `iamHost` – адрес (FQDN или имя устройства) Сервера администрирования, который включает IAM-компонент (начиная с Kaspersky Security Center Linux версии 16) и к которому подключается Kaspersky Security Center Web Console. Значение `iamHost` должно совпадать с адресом IAM, указанным при установке Сервера администрирования. Для получения указанного адреса IAM выполните следующую команду на устройстве с установленным Сервером администрирования: `grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` • `iamOAuthPort` – порт, который используется для обмена токенами аутентификации по протоколу аутентификации OpenID Connect (значение по умолчанию – 4444). Этот порт используется как для связи между Сервером Kaspersky Security Center Web Console и Сервером администрирования, так и между браузером (используется с Kaspersky Security Center Web Console) и Сервером администрирования. • `iamProxyPort` – порт, который используется для подключения Сервера Kaspersky Security Center Web Console к Серверу администрирования (значение по умолчанию – 9050). • `iamCertPath` – это путь к IAM-сертификату. IAM-сертификат создается автоматически при первом запуске Сервера администрирования. Сертификат хранится на устройстве, на котором установлен Сервер администрирования. Путь по умолчанию к сертификату: /var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem. Самоподписанный IAM-сертификат обновляется автоматически. • `iamPATPath` – путь к токену, который используется для регистрации Kaspersky Security Center Web Console в качестве OAuth-клиента в IAM. Этот файл создается автоматически при первом запуске Сервера администрирования. Токен хранится на устройстве, на котором установлен Сервер администрирования. Путь по умолчанию к токену: /var/opt/kaspersky/klnagent_srv/iam/initial_token.txt. Токен действует бессрочно и не требует ротации. • `kscPort` – порт, который используется для подключения Kaspersky Security Center Web Console к Серверу администрирования по OpenAPI (значение по умолчанию – 13299). • `kscCertPath` – путь к сертификату Сервера администрирования. Сертификат хранится на устройстве, на котором установлен Сервер администрирования. Путь по умолчанию к сертификату: /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer.	Секция файла JSON в следующем форм `"trusted": { "Administration Server v16": { "iamHost": "ksc-iam.example.com", "iamOAuthPort": 4444, "iamProxyPort": 9050, "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_c "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initia "kscPort": 13299, "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/ }, "Administration Server v15.4": { "kscHost": "ksc.example.com", "kscPort": 13299, "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/ } }`  Вы можете указать любые имена Серве администрирования вместо `Administr Server v16` и `Administration Serve`

Параметр	Описание	Доступные значения
	Для Сервера администрирования версии 15.4 и ниже: • имя Сервера администрирования, которое будет отображаться в окне входа. • `kscHost` – адрес (FQDN или имя устройства) Сервера администрирования, к которому подключается Kaspersky Security Center Web Console. • `kscPort` – порт OpenAPI, который используется для подключения Сервера Kaspersky Security Center Web Console к Серверу администрирования (значение по умолчанию – 13299). • `kscCertPath` – путь к сертификату Сервера администрирования. Сертификат хранится на устройстве, на котором установлен Сервер администрирования. Путь по умолчанию к сертификату: /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer. При установке Kaspersky Security Center Web Console на устройство, отличное от устройства Сервера администрирования, скопируйте файл сертификата Сервера администрирования (по пути, указанному в параметре `kscCertPath`), файл IAM-сертификата (по пути, указанному в параметре `iamCertPath`) и файл токена (по пути, указанному в параметре `iamPATPath`) с устройства, на котором установлен Сервер администрирования, на целевое устройство. Укажите локальный путь к этим файлам в файле ответов для установщика Web Console.	
`acceptEula`	Принимаете ли вы условия Лицензионного соглашения. Файл, содержащий условия Лицензионного соглашения, загружается вместе с установочным файлом.	Логическое значение: • `true` – Я подтверждаю, что полнос прочитал(а), понимаю и принимаю положения настоящего Лицензионн соглашения. • `false` – Я не принимаю условия Ли соглашения (выбрано по умолчани Если значение не указано, приложение Kaspersky Security Center Web Console Лицензионное соглашение и спросит, с принять условия Лицензионного согла
`certDomain`	Если вы хотите сгенерировать новый самоподписанный сертификат, используйте этот параметр, чтобы указать FQDN для подключения браузера к Kaspersky Security Center Web Console.	Строковое значение.
`certPath`	Используйте этот параметр, чтобы указать путь к пользовательскому сертификату Kaspersky Security Center Web Console, который является доверенным в вашей инфраструктуре и соответствует требованиям к пользовательским сертификатам. Вы можете указать только один закрытый ключ (`keyPath`) для одного сертификата или для цепочки сертификатов.	Строковое значение. Зашифрованные сертификаты не подде Kaspersky Security Center Web Console На устройстве, на котором установлен Kaspersky Security Center Web Console к файлу сертификата в формате кодиро Например: `/root/server.crt`
`keyPath`	Используйте этот параметр, чтобы задать путь к закрытому ключу, связанному с пользовательским сертификатом Kaspersky Security Center Web Console, указанным в параметре `certPath`.	Строковое значение. Файл с закрытым ключом не должен бы зашифрован. На устройстве, на котором установлен Kaspersky Security Center Web Console к файлу ключа в формате кодирования Например: `/root/key-without-passp`
`webConsoleAccount`	Имя учетной записи, под которой запущена служба Kaspersky Security Center Web Console.	Строковое значение следующего форм `группы >:< имя пользователя >"`. Например: `"Group1:User1"`. Если значение не указано, установщик Security Center Web Console создает п учетную запись `user_management_%ui`

Параметр	Описание	Доступные значения
`managementServiceAccount`	Имя учетной записи, под которой запущена служба Kaspersky Security Center Web Console Management Service.	Строковое значение следующего форм `группы >:< имя пользователя >"`. Например: `"Group1:User2"`. Если значение не указано, установщик Security Center Web Console создает п учетную запись `user_nodejs_%uid%`.
`serviceWebConsoleAccount`	Имя учетной записи, под которой запущена служба Kaspersky Security Center Web Console.	Строковое значение следующего форм `группы >:< имя пользователя >"`. Например: `"Group1:User3"`. Если значение не указано, установщик Security Center Web Console создает п учетную запись `user_svc_nodejs_%ui`
`pluginAccount`	Имя учетной записи, под которой запущена служба Kaspersky Security Center Product Plugins.	Строковое значение следующего форм `группы >:< имя пользователя >"`. Например: `"Group1:User4"`. Если значение не указано, установщик Security Center Web Console создает п учетную запись `user_web_plugin_%ui`
`natsMessageQueueAccount`	Имя учетной записи, под которой запущена служба Kaspersky Security Center Web Console NATS.	Строковое значение следующего форм `группы >:< имя пользователя >"`. Например: `"Group1:User6"`. Если значение не указано, установщик Security Center Web Console создает п учетную запись `user_message_queue_`
`internalCertsTTLDays`	Срок действия внутренних сертификатов Kaspersky Security Center Web Console.	Необязательный параметр. Значение по равно 1095.

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

В этом разделе описано, как установить Сервер Kaspersky Security Center Web Console (далее также Kaspersky Security Center Web Console) на устройства с операционной системой Astra Linux Special Edition. Сначала необходимо установить СУБД и Сервер администрирования Kaspersky Security Center Linux.

Чтобы установить Kaspersky Security Center Web Console:

1. Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center Web Console, работает один из поддерживаемых дистрибутивов Linux.

2. Прочитайте Лицензионное соглашение. Если в состав дистрибутива Kaspersky Security Center Linux 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 приложение.

3. Создайте файл ответов, который содержит параметры для подключения Kaspersky Security Center Web Console к Серверу администрирования: `/etc/ksc-web-console-setup.json`.

   Пример файла ответов с минимальным набором параметров

Набор параметров файла ответов зависит от версии Сервера администрирования, к которому подключено приложение Kaspersky Security Center Web Console:

- Сервер администрирования версии 16 и выше

  Пример файла ответов с минимальным набором параметров для входа на Сервер администрирования версии 16 и выше:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Сервер администрирования версии 15.4 и выше

  Пример файла ответов с минимальным набором параметров для входа на Сервер администрирования версии 15.4 и ниже:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Вы можете установить Kaspersky Security Center Web Console на том же устройстве, что и Сервер администрирования, или на другом устройстве. Если приложение Kaspersky Security Center Web Console установлено на другом устройстве, адрес Kaspersky Security Center Web Console (параметр `address`) и адрес Сервера администрирования (параметр `iamHost` или `kscHost`) отличаются. Если приложение Kaspersky Security Center Web Console установлено на одном устройстве с Сервером администрирования, эти параметры имеют одинаковые значения.

Значение `iamHost` должно совпадать с адресом IAM, который вы указали при установке Сервера администрирования. Для получения указанного адреса IAM выполните следующую команду на устройстве с установленным Сервером администрирования:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Подробную информацию см. в статье Параметры установки Kaspersky Security Center Web Console.

Вы можете добавить несколько Серверов администрирования разных версий в список доверенных серверов. В этом случае Серверы могут использовать разные способы аутентификации.

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

```
DIGSIG_ELF_MODE=1
```

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

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

6. Создайте директорию для ключа приложения:

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

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

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

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

8. Обновите оперативную память дисков:

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

Перезагрузите систему.

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

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

```
sudo apt-get install ksc-web-console-<номер_сборки>.x86_64.deb
```

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

```
sudo apt-get install ksc-web-console-<номер_сборки>.x86_64.deb
```

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

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

```
sudo systemctl restart KSC*
```

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

Установка Kaspersky Security Center Linux с помощью скрипта

Скрипт `ksc_fast_install.py` позволяет вам развернуть Kaspersky Security Center Linux и выполнить первоначальную настройку его компонентов: Сервера администрирования и Web Console, включая СУБД и необходимые пакеты.

Скрипт получает параметры из файла параметров. Скрипт использует значения параметров по умолчанию. Если необходимо, вы можете изменить значения.

Как работает скрипт

Во время работы скрипт выполняет следующее:

- Проверяет выполнение условий:
  - У вас есть необходимые права для выполнения скрипта.
  - Скрипт совместим с операционной системой и СУБД.
  - Условия Лицензионное соглашения и Политики конфиденциальности приняты.

    Если вы не приняли их в файле параметров, вам будет предложено сделать это после запуска скрипта.
  - Аппаратные требованиях к Серверу администрирования и Web Console.

    Требования определены в Руководстве по масштабированию.
- Устанавливает СУБД (если еще не установлена) и настраивает ее параметры.
- Создает базы Kaspersky Security Center, настраивает учетные данные операционной системы.
- Устанавливает Сервер администрирования, Web Console.
- Предоставляет вам учетную запись и пароль для входа в Web Console.

  Прежде чем закрыть терминал командной строки, сохраните учетные данные любым удобным способом. Если вы потеряете учетные данные, вам нужно добавить новую учетную запись пользователя, выполнив команду: `` `/opt/kaspersky/ksc64/sbin/kladduser -n <пользователь>` ``

Если одно или несколько условий не выполнено или возникает ошибка, скрипт завершается и отображается соответствующее уведомление.

В скрипте не предусмотрены действия по усилению защиты системы. Чтобы снизить риск компрометации Kaspersky Security Center, ознакомьтесь с рекомендациями Руководства по усилению защиты.
Способ установки с помощью скрипта применим для развертывания Kaspersky Security Center Linux версии 16.3 и выше на устройстве без Kaspersky Security Center Linux.
Для запуска скрипта требуется Python 3.6 или выше.

Развертывание возможно только на устройстве, на котором не установлен Kaspersky Security Center Linux.

Вы не можете использовать скрипт для обновления Kaspersky Security Center Linux до новой версии или если развернут отказоустойчивый кластер Kaspersky Security Center Linux.

Скрипт `ksc_fast_install.py` поддерживает установку Kaspersky Security Center Linux на версии операционных систем с СУБД, описанных в таблице.

Версия операционной системы.	СУБД
Ubuntu Server 26.04 LTS	PostgreSQL 18 MySQL 8.4 (сборка 8.4.10)
РЕД ОС 8	PostgreSQL 16 MariaDB 10.11 (сборка 10.11.18)
Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8.5)	PostgreSQL 15 MariaDB 10.11 (сборка 10.11.13)
CentOS Stream 10	PostgreSQL 18 MariaDB 10.11 (сборка 10.11.13)

Пользовательская схема базы данных не поддерживается.

Как выполнить развертывание с помощью скрипта

Предварительные требования

Прежде чем запустить скрипт, убедитесь, что вы выполнили следующее:

- Обновите операционную систему, выполнив одну из команд: `dnf update` или `apt update`
- Получите права суперпользователя, выполнив команду: `sudo -i`
- Разрешите запуск скрипта, выполнив команду: `chmod +x ./ksc_fast_install.py`
- Убедитесь, что в хранилищах вашей операционной системы доступна поддерживаемая СУБД, выполнив команду: `sudo apt policy postgresql`

Чтобы развернуть Kaspersky Security Center Linux с помощью скрипта:

1. С сайта "Лаборатории Касперского", скачайте следующее:
   - Дистрибутивы .deb или .rpm для Сервера администрирования и Web Console.
   - Архив "KSC installation script".

   При использовании скрипта выберите дистрибутивы Сервера администрирования и Web Console, совместимые с диспетчером пакетов вашей операционной системы.

В архиве находятся следующие файлы:

- Файл скрипта `ksc_fast_install.py`.
- Файл параметров.

  Имя файла по умолчанию – `params.txt`. Если вы хотите переименовать файл, убедитесь, что вы указали новое имя через параметр `--params` при запуске скрипта в терминале командной строки.
- Файл с Лицензионным соглашением и Политикой конфиденциальности для Сервера администрирования.
- Файл с Лицензионным соглашением для Kaspersky Security Center Web Console.
- Файлы с хеш-суммами Лицензионных соглашений.

2. Поместите все скачанные файлы в одну локальную директорию.
3. При необходимости настройте файл параметров.

Нажмите здесь, чтобы просмотреть пример файла параметров с описанием параметров

```
# Required parameters:

#klfi_server_eula_accepted=N

#klfi_nwc_eula_accepted=N

#klfi_pp_accepted=N

# Optional parameters:

#klfi_klserver_db=KAV

#klfi_klserver_dbuser=klserver

#klfi_klserver_address=

#klfi_kliam_db=KAV_IAM

#klfi_kliam_dbuser=kliam

#klfi_kliam_address=

#klfi_sys_group_kladmin=kladmins

#klfi_sys_user_klserver=klsrvuser

#klfi_sys_user_kliam=kliamuser

#klfi_sys_user_svc=klsvcuser

#klfi_nwc_port=8080

#klfi_display_name=
```

#klfi_netsize=M

Параметры klfi_server_eula_accepted=N ,klfi_nwc_eula_accepted=N иklfi_pp_accepted=N являются обязательными и всегда есть в файле параметров. Остальные параметры необязательны.

Для обязательных параметров:

- Если вы измените значение по умолчанию, не раскомментировав строку, вам будет предложено принять Лицензионное соглашение и Политику конфиденциальности.
- Если вы укажете значение отличное от Y или N, вам будет предложено принять Лицензионное соглашение и Политику конфиденциальности независимо от того, раскомментировали ли вы строку.
- Если вы раскомментируете строку, не изменив значение по умолчанию N, скрипт не будет работать.
- Если вы раскомментируете строку и установите значение Y, скрипт не предложит принять Лицензионное соглашение и Политику конфиденциальности.

Параметр и его значение по умолчанию	Описание параметра и другие возможные значения (если есть)
klfi_server_eula_accepted=N	Лицензионное соглашение для Сервера администрирования. Возможные значения: • Y – Лицензионное соглашение принято. • N – Лицензионное соглашение не принято.
klfi_nwc_eula_accepted=N	Лицензионное соглашение для Kaspersky Security Center Web Console. Возможные значения: • Y – Лицензионное соглашение принято. • N – Лицензионное соглашение не принято.
klfi_pp_accepted=N	Политика конфиденциальности. Возможные значения: • Y – Политика конфиденциальности принята. • N – Политика конфиденциальности не принята.
klfi_klserver_db=KAV	Имя базы данных Сервера администрирования. Имя должно отличаться от имени базы данных IAM, указанного в параметре klfi_kliam_db.
klfi_kliam_db=KAV_IAM	Имя базы данных IAM. Имя должно отличаться от имени базы данных Сервера администрирования, указанного в параметре klfi_klserver_db.
klfi_klserver_dbuser=klserver	Имя пользователя базы данных Сервера администрирования.
klfi_kliam_dbuser=kliam	Имя пользователя базы данных IAM.
klfi_klserver_address=FQDN	FQDN Сервера администрирования или текущее имя устройства. Если значение параметра не указано, скрипт автоматически определяет FQDN или имя устройства, на котором вы запускаете скрипт. Если скрипту не удается определить значения, установка завершается с ошибкой.
klfi_kliam_address=FQDN	FQDN сервера IAM или текущее имя устройства. Если значение параметра не указано, скрипт автоматически определяет FQDN или имя устройства, на котором вы запускаете скрипт. Если скрипту не удается определить значения, установка завершается с ошибкой.
klfi_sys_group_kladmin=kladmins	Имя группы безопасности для служб.
klfi_sys_user_klserver=klsrvuser	Имя учетной записи для запуска службы Сервера администрирования.
klfi_sys_user_kliam=kliamuser	Имя учетной записи для запуска службы IAM.

`klfi_sys_user_svc=klsvcuser`	Имя учетной записи для запуска других служб.
`klfi_nwc_port=8080`	Порт для подключения к Kaspersky Security Center Web Console.
`klfi_display_name=FQDN`	имя Сервера администрирования, которое будет отображаться в окне входа.

`klfi_netsize=M`	Примерное количество устройств, которыми вы планируете управлять.
	Каждая оценка учитывает ресурсы, необходимые для запуска приложений "Лаборатории Касперского". Расчет охватывает одновременную работу Сервера администрирования, Агента администрирования, Kaspersky Security Center Web Console и Kaspersky Endpoint Security для Linux на одном устройстве.
	Хранилище резервных копий Сервера администрирования в эти расчеты не входит. Используйте внешний файловый ресурс в качестве точки монтирования для хранения резервных копий на отдельном устройстве или увеличьте доступное дисковое пространство для учета хранилища резервных копий.
	Рекомендуется добавить дополнительно оперативной памяти 4–6 ГБ и 20 ГБ свободного места на диске для установки операционной системы.
	Оценка аппаратных ресурсов по размеру сети:
	• `S` – от 1 до 1000 управляемых устройств.
	  • Процессор – 8 ядер.
	  • Оперативная память – 16 ГБ.
	  • Объем свободного места на диске для директории `/var` – 70 ГБ, 300 IOPS и выше.
	• `M` – от 1001 до 10000 управляемых устройств.
	  • Процессор – 12 ядер.
	  • Оперативная память – 24 ГБ.
	  • Объем свободного места на диске для директории `/var` – 340 ГБ, 300 IOPS и выше.
	• `L` – от 10 001 до 30 000 управляемых устройств.
	  • Процессор – 20 ядер.
	  • Оперативная память – 40 ГБ.
	  • Объем свободного места на диске для директории `/var` – 490 ГБ, 300 IOPS и выше.
	• `XL` – от 30 000 до 50 000 управляемых устройств.
	  • Процессор – 28 ядер.
	  • Оперативная память – 54 ГБ.
	  • Объем свободного места на диске для директории `/var` – 640 ГБ, 300 IOPS и выше.

Строки файла параметров закомментированы. Если вы хотите настроить значения, удалите символ # в начале строки, которую вы хотите раскомментировать.

Параметры `klfi_server_eula_accepted`, `klfi_nwc_eula_accepted` и `klfi_pp_accepted` являются обязательными и их значение по умолчанию – `N`. Если запустить скрипт, не изменив эти значения в файле параметров, вам будет предложено подтвердить принятие Лицензионного соглашения и Политики конфиденциальности.

4. Запустите скрипт.

   После выполнения скрипта отображается уведомление об успешном развертывании компонентов Kaspersky Security Center Linux, а также учетная запись и пароль для входа в Web Console.

Если условия для установки с помощью скрипта не выполняются, в файле параметров указаны неизвестные параметры или если параметр повторяется несколько раз, скрипт возвращает ошибку и отображается соответствующее уведомление.

Если сценарий неправильно обнаруживает нехватку оперативной памяти на этапе обнаружения ресурсов, выключите динамическое использование оперативной памяти на время установки.

Если при установке компонентов Kaspersky Security Center Linux или СУБД возникает ошибка, скрипт откатывает изменения и завершает работу.

Откат неудачной установки

Если при установке компонентов Kaspersky Security Center Linux или СУБД возникает ошибка, откат обновления выполняется скриптом автоматически. Компонент или СУБД, установленные до возникновения ошибки, удаляются.

Обновление пакетов операционной системы и установка пакетов не откатываются.

Если вы вручную завершите выполнение скрипта, успешно выполненные шаги не будут отменены. При следующем запуске скрипта (с помощью команды `python3 ksc_fast_install.py`) установка возобновится с шага, на котором она была прервана. Если вы не хотите возобновлять установку, запустите скрипт с параметром `rollback`: `python3 ksc_fast_install.py rollback.` Скрипт откатит все действия, выполненные до завершения его работы.

Развертывание отказоустойчивого кластера Kaspersky Security Center Linux

Отказоустойчивый кластер Kaspersky Security Center Linux обеспечивает высокую доступность Kaspersky Security Center Linux и минимизирует простои Сервера администрирования в случае сбоя. Отказоустойчивый кластер основан на двух идентичных экземплярах Kaspersky Security Center Linux, 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.

Отказоустойчивый кластер Kaspersky Security Center Linux поддерживает две конфигурации:

- отказоустойчивый кластер, узлы которого расположены в едином центре обработки данных;
- геораспределенный отказоустойчивый кластер, узлы которого расположены в разных центрах обработки данных.

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

Используйте функцию syslog для устранения неполадок.

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.
- Хотя бы одна из служб (или процессов) Kaspersky Security Center Linux завершилась с ошибкой или была случайно остановлена. К службам Kaspersky Security Center Linux относятся: klnagent_klfoc, kladminserver_klfoc, klactprx_klfoc, klwebsrv_klfoc.
- Сетевое соединение между активным узлом и хранилищем на файловом сервере было прервано или разорвано (только для кластера, расположенного в одном центре обработки данных).

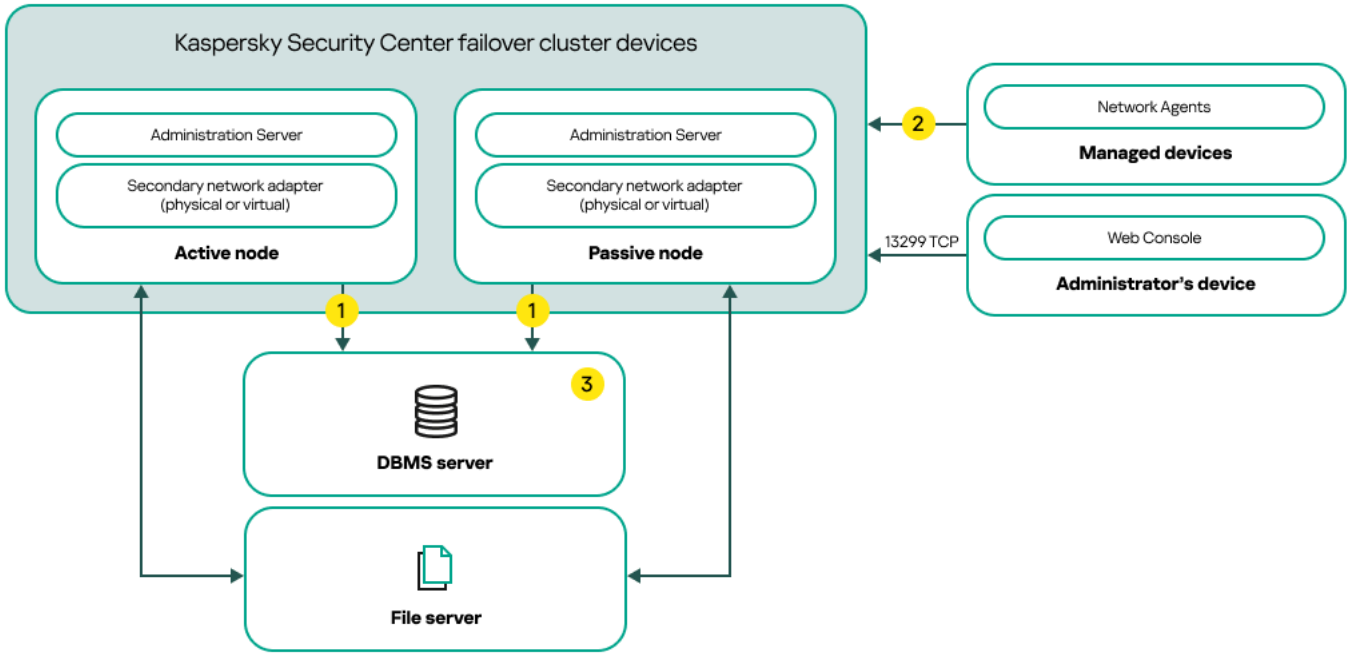
Отказоустойчивый кластер Kaspersky Security Center Linux. Схемы развертывания

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

- Отказоустойчивый кластер Kaspersky Security Center Linux, развернутый в одном центре обработки данных:
  - Схема, которая использует дополнительный сетевой адаптер и СУБД, установленную на выделенном устройстве.
  - Схема, которая использует сторонний балансировщик нагрузки и СУБД, установленную на выделенном устройстве.
- Геораспределенный отказоустойчивый кластер Kaspersky Security Center Linux, развернутый в нескольких центрах обработки данных.

Отказоустойчивый кластер Kaspersky Security Center Linux

Схема, которая использует дополнительный сетевой адаптер и СУБД, установленную на выделенном устройстве



Схема, которая использует дополнительный сетевой адаптер и СУБД, установленную на выделенном устройстве

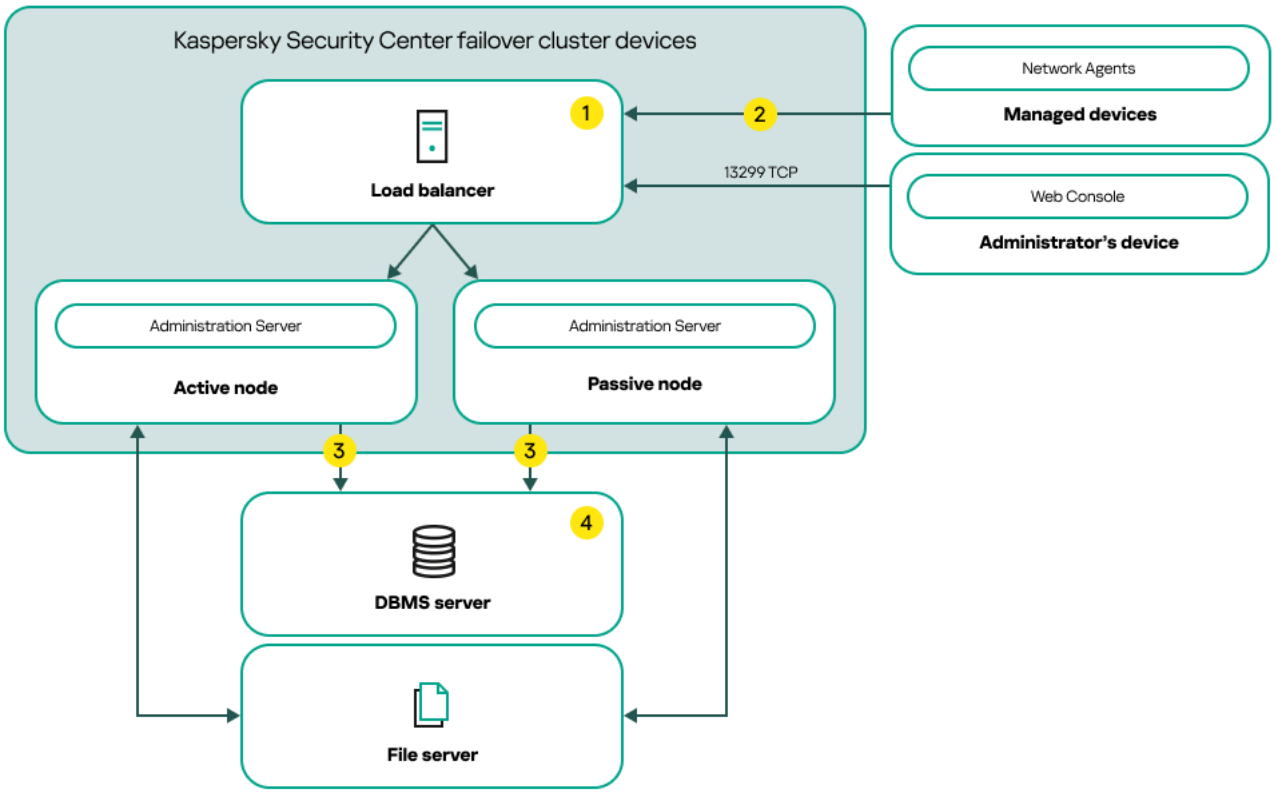
Условные обозначения схемы:

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 Откройте следующие порты на устройствах с Сервером администрирования для подключения к управляемым устройствам: 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.

Схема, которая использует сторонний балансировщик нагрузки и СУБД, установленную на выделенном устройстве



Схема, которая использует сторонний балансировщик нагрузки и СУБД, установленную на выделенном устройстве

Условные обозначения схемы:

1 На устройстве балансировщика 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 нужно открыть TCP-порт 13291.

2 Откройте следующие порты на устройствах с Сервером администрирования для подключения к управляемым устройствам: 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.

Геораспределенный отказоустойчивый кластер Kaspersky Security Center Linux

Такая схема развертывания позволяет обеспечить отказоустойчивость всех компонентов. В этой схеме Сервер администрирования, СУБД и Kaspersky Security Center Web Console установлены на обоих узлах кластера.

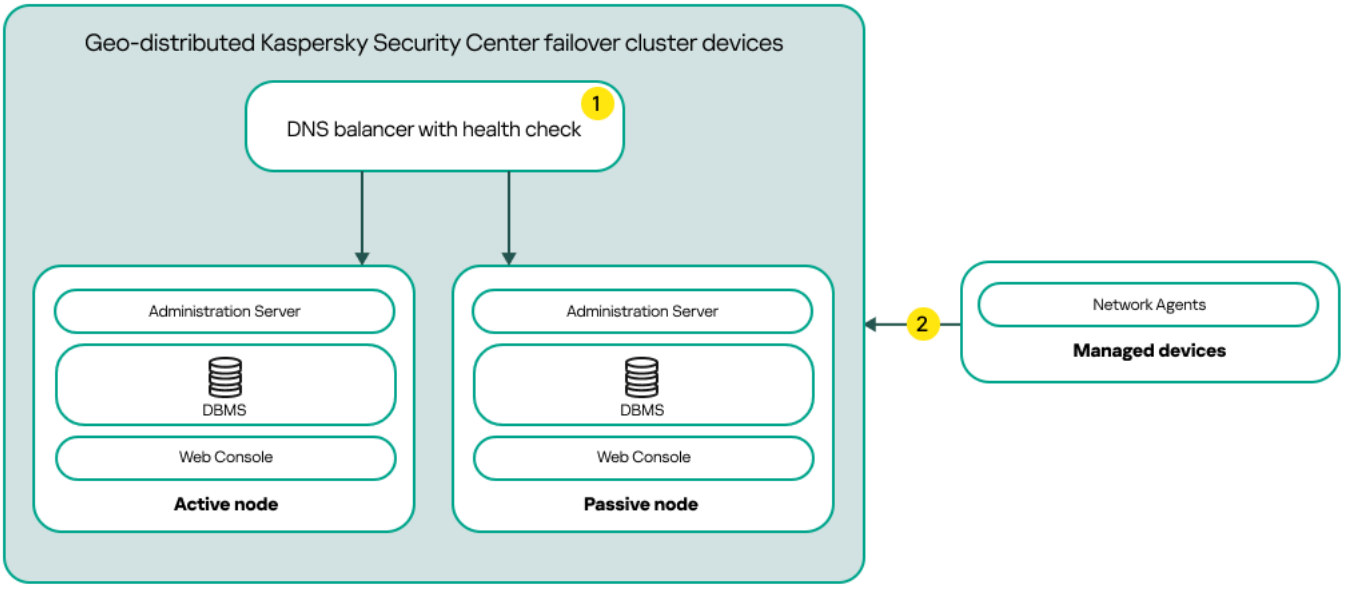


Схема развертывания геораспределенного отказоустойчивого кластера Kaspersky Security Center Linux

1 DNS-балансировщик с проверкой работоспособности, который необходимо развернуть на вашей стороне перед установкой геораспределенного отказоустойчивого кластера Kaspersky Security Center Linux.

DNS-балансировщик периодически проверяет состояние узлов кластера. При доступе к кластеру по его доменному имени DNS-балансировщик всегда возвращает IP-адрес активного узла.

2 Откройте следующие порты на устройствах с Сервером администрирования для подключения к управляемым устройствам: TCP 13000, UDP 13000 и TCP 17000.

Отказоустойчивый кластер Kaspersky Security Center Linux

Этот раздел содержит общую информацию об отказоустойчивом кластере Kaspersky Security Center Linux, развернутом в рамках одного центра обработки данных, 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 Linux обеспечивает высокую доступность Kaspersky Security Center Linux и минимизирует простои Сервера администрирования в случае сбоя. Отказоустойчивый кластер основан на двух идентичных экземплярах Kaspersky Security Center Linux, 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.

Развертывание приложений "Лаборатории Касперского" состоит из следующих этапов:

> Рекомендуется соблюдать последовательность этапов, которая описана в этом сценарии.

1. **Проверка аппаратных требований**

   Убедитесь, что у вас есть оборудование, соответствующее требованиям для отказоустойчивого кластера.

2. **Выбор схемы развертывания**

   Выберите схему развертывания. Это влияет на следующие этапы развертывания.

3. **Подготовка учетных записей пользователей для служб Kaspersky Security Center Linux**

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

   1. Создайте группу `kladmins`. Выполните следующие команды:

      ```
      sudo groupadd kladmins
      ```

      ```
      sudo groupmod -g <новый_GID> kladmins
      ```

      Убедитесь, что у этой группы одинаковый GID на всех трех устройствах. Выполните следующую команду:

      ```
      getent group kladmins
      ```

      Если идентификаторы GID не совпадают, вы можете использовать следующую команду, чтобы указать GID:

      ```
      sudo groupmod -g <новый_GID> kladmins
      ```

   2. Создайте учетную запись `ksc`. Назначьте учетные записи пользователей группе `kladmins`. Выполните следующие команды:

      ```
      sudo adduser ksc
      ```

      ```
      sudo usermod -u <новый_UID> ksc
      ```

      ```
      sudo gpasswd -a ksc kladmins
      ```

      ```
      sudo usermod -g kladmins ksc
      ```

      Убедитесь, что у этой учетной записи пользователя одинаковый UID на всех трех устройствах. Выполните следующую команду:

      ```
      getent passwd ksc
      ```

      Если идентификаторы UID не совпадают, вы можете использовать следующую команду, чтобы указать UID:

```
sudo usermod -u <новый_UID> ksc
```

3. Создайте учетную запись пользователя `rightless`. Назначьте учетные записи пользователей группе `kladmins`. Выполните следующие команды:

   ```
   sudo adduser rightless
   ```

   ```
   sudo usermod -u <новый_UID> rightless
   ```

   ```
   sudo gpasswd -a rightless kladmins
   ```

   ```
   sudo usermod -g kladmins rightless
   ```

   Убедитесь, что у этой учетной записи пользователя одинаковый UID на всех трех устройствах. Выполните следующую команду:

   ```
   getent passwd rightless
   ```

   Если идентификаторы UID не совпадают, вы можете использовать следующую команду, чтобы указать UID:

   ```
   sudo usermod -u <новый_UID> rightless
   ```

4. Создайте учетную запись пользователя `ksciam`. Назначьте учетные записи пользователей группе `kladmins`. Выполните следующие команды:

   ```
   sudo adduser ksciam
   ```

   ```
   sudo usermod -u <новый_UID> ksciam
   ```

   ```
   sudo gpasswd -a ksciam kladmins
   ```

   ```
   sudo usermod -g kladmins ksciam
   ```

   Убедитесь, что у этой учетной записи пользователя одинаковый UID на всех трех устройствах. Выполните следующую команду:

   ```
   getent passwd ksciam
   ```

   Если идентификаторы UID не совпадают, вы можете использовать следующую команду, чтобы указать UID:

   ```
   sudo usermod -u <новый_UID> ksciam
   ```

5. При необходимости увеличьте установленное по умолчанию максимальное количество файлов, которые можно открывать (файловые дескрипторы) для учетных записей, используемых для работы служб Kaspersky Security Center Linux. Для этого откройте файл /etc/security/limits.conf и укажите мягкие и жесткие ограничения файловых дескрипторов следующим образом:

   ```
   ksc soft nofile <максимальное_количество_открытых_файлов>
   ```

   ```
   ksc hard nofile <максимальное_количество_открытых_файлов>
   ```

   По умолчанию ограничения дескрипторов файлов указываются во время установки. Мягкие ограничения файлов составляют 32 768 файлов, жесткие ограничения файлов составляют 131 072 файла.

4 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 Linux и настройте права доступа к общим папкам.

Инструкции: Подготовка файлового сервера для отказоустойчивого кластера Kaspersky Security Center Linux.

5 Установка СУБД

Установите СУБД для Kaspersky Security Center Linux. Вы можете выбрать одну из поддерживаемых СУБД. Подробнее о том как установить выбранную СУБД, см. в документации к этой СУБД.

Если дистрибутив вашей операционной системы на базе Linux не содержит поддерживаемую СУБД, вы можете установить СУБД из стороннего хранилища пакетов.

После установки СУБД выполните соответствующую инструкцию:

- Настройка сервера PostgreSQL или Postgres Pro для работы с Kaspersky Security Center Linux
- Настройка сервера MariaDB x64 для работы с Kaspersky Security Center Linux

Создайте вручную базу данных для IAM. Сервер администрирования не удаляет базу данных IAM автоматически при деинсталляции или переносе Сервера на другое устройство, требуется удалить базу данных вручную.

- Для PostgreSQL выполните команду:

  ```
  sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
  ```

- Для MariaDB выполните команду:

  ```
  sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
  ```

На устройстве с установленной СУБД настройте подключение к устройствам, которые будут работать как активные и пассивные узлы.

6 **Подготовка активного и пассивного узлов**

Подготовьте два устройства с одинаковым аппаратным и программным обеспечением для работы в качестве активного и пассивного узлов.

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

7 **Установка Kaspersky Security Center Linux**

Установите Kaspersky Security Center Linux в режиме отказоустойчивого кластера на оба узла.

Сначала необходимо установить Kaspersky Security Center Linux на устройство, которое вы хотите использовать в качестве активного узла, а затем установить его на пассивный узел.

Инструкции: Установка Kaspersky Security Center Linux на узлы отказоустойчивого кластера Kaspersky Security Center Linux.

8 **Установка Kaspersky Security Center Web Console**

Установите Kaspersky Security Center Web Console на отдельном устройстве, не являющемся узлом кластера.

Укажите отказоустойчивый кластер в качестве адреса Сервера администрирования в файле ответов.

Сертификат Сервера администрирования находится по следующему пути: /mnt/KlFocDataShare_klfoc/1093/cert/klserver.cer.

Скопируйте файл сертификата на устройство, на котором будет установлен Kaspersky Security Center Web Console. Укажите локальный путь к сертификату в файле ответов.

9 **Тестирование отказоустойчивого кластера**

Убедитесь, что вы правильно настроили отказоустойчивый кластер и правильно ли он работает. Например, вы можете выполнить следующую команду, чтобы инициировать переключение на пассивный узел:

```
/opt/kaspersky/ksc64/sbin/klfoc -failover --stp klfoc
```

Используйте следующую команду, чтобы убедиться, что служба управления отказоустойчивым кластером находится в состоянии `Active: active (running)` на обоих узлах:

`systemctl status klfocsvc_klfoc`

Используйте следующие команды, чтобы убедиться, что другие службы отказоустойчивого кластера находятся в состоянии `Active: active (running)` на активном узле. На пассивном узле эти службы отказоустойчивого кластера должны быть в состоянии `Active: inactive (dead)` или `Active: failed (Result: signal)`.

- `systemctl status klnagent_klfoc`
- `systemctl status kladminserver_klfoc`
- `systemctl status klactprx_klfoc`
- `systemctl status klwebsrv_klfoc`

Отказоустойчивый кластер Kaspersky Security Center Linux развернут.

Отказоустойчивый кластер Kaspersky Security Center Linux. Аппаратные и программные требования

После установки Сервера администрирования на устройство рекомендуется установить Kaspersky Endpoint Security для Linux.
Для совместной установки у вас должно быть не менее 300 IOPS, а также нужно добавить к требованиям Сервера администрирования 1,5 ГБ ОЗУ и 15% к требованиям процессора.
Требования к оборудованию для Kaspersky Endpoint Security см. в справке Kaspersky Endpoint Security для Linux.

Информацию о параметрах безопасности, необходимых для работы с Kaspersky Security Center Linux, см. в справке Kaspersky Endpoint Security для Linux.

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.

  Минимальная конфигурация для активных и пассивных узлов

Оборудование	Значение
Процессор	2 ядра, 2500 МГц
ОЗУ	6 ГБ
Дисковое пространство	10 ГБ, 150 IOPS или выше
Контроллер интерфейса сети	1 Гбит/сек

  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.

  Требования к конфигурации активных и пассивных узлов в зависимости от количества управляемых устройств доступны в статье Аппаратные требования для СУБД и Сервера администрирования.

- Устройство, на котором будет установлена Kaspersky Security Center Linux Web Console.

  Конфигурация устройства для работы 10 и менее системных администраторов

Оборудование	Значение
Процессор	2 ядра, 2500 МГц
ОЗУ	4 ГБ
Дисковое пространство	40 ГБ, 150 IOPS или выше

  Конфигурация устройства для работы более 10 системных администраторов

Оборудование	Значение
Процессор	4 ядра, 2500 МГц
ОЗУ	8 ГБ
Дисковое пространство	40 ГБ, 150 IOPS или выше

- Файловый сервер, поддерживающий протокол CIFS/SMB версии 2.0 или выше. Вам нужно выделить отдельное устройство, которое будет выступать в качестве файлового сервера.

  Конфигурация файлового сервера

Оборудование	Значение
Процессор	4 ядра, 2500 МГц
ОЗУ	32 ГБ
Дисковое пространство	500 ГБ, 500 IOPS или выше
Контроллер интерфейса сети	10 Гбит/сек

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

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

- Устройство балансировщика нагрузки. Используется в схеме развертывания отказоустойчивого кластера Kaspersky Security Center Linux, которая использует сторонний балансировщик нагрузки и СУБД, установленную на выделенном устройстве.

  Конфигурация устройства балансировщика нагрузки Nginx

Оборудование	Значение
Процессор	2 ядра, 2500 МГц
ОЗУ	4 ГБ

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.

   В зависимости от вашего дистрибутива Linux установите либо пакет nfs-utils, либо пакет nfs-kernel-server, выполнив соответствующую команду:

   ```
   sudo yum install nfs-utils
   sudo apt install nfs-kernel-server
   ```

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 Linux. Вам нужно будет указать пути к общим папкам при установке Kaspersky Security Center Linux.

   Убедитесь, что не существуют следующие папки:

   - `/mnt/KlFocStateShare`
   - `/mnt/KlFocDataShare_klfoc`

   Если какая-либо из этих папок существует, рекурсивно удалите ее.

   Выполните следующие команды:

   ```
   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 770 /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 exportfs -a
   sudo systemctl start rpcbind
   sudo systemctl start nfs-server
   ```

   Включите автозапуск, выполнив следующую команду:

   ```
   sudo systemctl enable rpcbind
   ```

Вы можете указать пользовательские папки, но рекомендуется использовать предложенные имена папок для удобства при использовании справки.

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

Прежде чем продолжить, убедитесь, что вы выполнили предыдущие шаги сценария Развертывание отказоустойчивого кластера "Лаборатории Касперского".

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

Конфигурация общих папок

Чтобы настроить общие папки:

1. В зависимости от вашего дистрибутива Linux установите либо пакет nfs-utils, либо пакет nfs-kernel-server на каждом узле, выполнив соответствующую команду:

   `yum install nfs-utils`

   `apt install nfs-kernel-server`

2. Создайте точки монтирования, выполнив следующие команды:

   `mkdir -p /mnt/KlFocStateShare`

   `mkdir -p /mnt/KlFocDataShare_klfoc`

3. Сопоставьте точки монтирования и общие папки:

   `sudo sh -c "echo <файловый сервер>:/mnt/KlFocStateShare /mnt/KlFocStateShare nfs vers=4,soft,timeo=50,retrans=2,auto,user,rw 0 0 >> /etc/fstab"`

   `sudo sh -c "echo <файловый сервер>:/mnt/KlFocDataShare_klfoc /mnt/KlFocDataShare_klfoc nfs vers=4,noauto,user,rw,exec 0 0 >> /etc/fstab"`

   Где `{файловый сервер}` – это FQDN файлового сервера с общими папками.

4. Подключите общие папки, выполнив следующие команды:

   `mount /mnt/KlFocStateShare`

   `mount /mnt/KlFocDataShare_klfoc`

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

   Выполните следующую команду:

   `ls -la /mnt/`

Конфигурация сетевого адаптера

Дополнительный сетевой адаптер может быть физическим или виртуальным. Если вы выбрали схему развертывания с дополнительным сетевым адаптером, выполните соответствующую процедуру на обоих узлах:

- Используйте виртуальный дополнительный сетевой адаптер на основе физического сетевого адаптера (технология MACVLAN):

  1. Установите пакет iputils-arping. В зависимости от вашего дистрибутива Linux выполните одну из следующих команд:

     - `yum install iputils`

     Или

     - `apt install iputils-arping`

  2. Чтобы убедиться, что NetworkManager используется для управления физическим сетевым адаптером, выполните следующую команду:

     `nmcli device status`

     Если вывод команды показывает, что физический сетевой адаптер не управляется, настройте NetworkManager для управления физическим сетевым адаптером. Точные шаги настройки зависят от вашего дистрибутива Linux.

  3. Чтобы идентифицировать интерфейсы, используйте следующую команду:

     `ip a`

  4. Чтобы создать конфигурационный профиль, выполните следующую команду:

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

- Используйте физический дополнительный сетевой адаптер или создайте виртуальное устройство TAP с помощью гипервизора. В этом случае выключите приложение NetworkManager.

  1. Подключите дополнительный сетевой адаптер к узлу.

  2. Установите пакет iputils-arping. В зависимости от вашего дистрибутива Linux выполните одну из следующих команд:

     - `yum install iputils`

     Или

     - `apt install iputils-arping`

  3. Чтобы удалить подключение NetworkManager для целевого интерфейса, выполните следующую команду:

     `nmcli con del <название соединения>`

     Чтобы проверить подключения с целевым интерфейсом, выполните следующую команду:

     `nmcli con show`

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

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

5. Перезагрузите NetworkManager:

   ```
   systemctl reload NetworkManager
   ```

   Чтобы убедиться, что целевой интерфейс больше не управляется, выполните следующую команду:

   ```
   nmcli dev status
   ```

Конфигурация балансировщика нагрузки

Если вы выбрали схему развертывания с балансировщиком нагрузки, следуйте инструкциям ниже, чтобы настроить его.

Чтобы настроить балансировщик нагрузки:

1. Подготовьте выделенное Linux-устройство с установленным nginx или другим балансировщиком нагрузки.
2. Настройте балансировку нагрузки. Установите активный узел в качестве основного сервера и пассивный узел в качестве резервного сервера.
3. На сервере nginx откройте все порты Сервера администрирования в соответствии со статьей Порты, используемые Kaspersky Security Center Linux.

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

> Доступность узлов отказоустойчивого кластера должна определяться доступностью основных портов подключения к Серверу администрирования. Пассивный узел не принимает никаких внешних подключений, пока не произойдет переключение.

Установка Kaspersky Security Center Linux на узлы отказоустойчивого кластера Kaspersky Security Center Linux

Прежде чем продолжить, убедитесь, что вы выполнили предыдущие шаги сценария Развертывание отказоустойчивого кластера "Лаборатории Касперского".

Эта процедура описывает, как установить Kaspersky Security Center Linux на узлы отказоустойчивого кластера Kaspersky Security Center Linux. Kaspersky Security Center Linux устанавливается на оба узла отказоустойчивого кластера Kaspersky Security Center Linux по отдельности. Сначала вы устанавливаете приложение на активный узел, затем на пассивный. Во время установки вы выбираете, какой узел будет активным, а какой пассивным.

В зависимости от дистрибутива Linux, установленного на вашем устройстве, вам нужно использовать один из следующих установщиков:

- ksc64_[номер_версии]_amd64.deb
- ksc64-[номер_версии].x86_64.rpm

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

Если вы используете РЕД ОС версии 7.3.4 и выше или МСВСфера версии 9.2 и выше, вам нужно установить пакет libxcrypt-compat на обоих узлах.

Установка на активный узел

Чтобы установить Kaspersky Security Center Linux на активном узле:

1. Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center Linux, работает один из поддерживаемых дистрибутивов Linux.

2. Если вы используете дополнительный сетевой адаптер, введите его имя при появлении запроса. Вы можете выполнить следующую команду, чтобы отобразить все сетевые интерфейсы:

   ```
   ip addr
   ```

3. Запустите установку Kaspersky Security Center Linux. В зависимости от вашего дистрибутива Linux выполните одну из следующих команд:

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

4. Запустите настройку Kaspersky Security Center Linux:

   ```
   /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 Linux, вам нужно 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) в соответствии с Политикой конфиденциальности. Введите `n`, если вы не принимаете условия Политики конфиденциальности. Чтобы использовать Kaspersky Security Center Linux, вам нужно принять условия Политики конфиденциальности.

6. Выберите значение **Управляющий узел кластера**, в качестве режима установки Сервера администрирования.

7. При отображении запроса укажите следующие параметры:

   a. Введите локальный путь к точке монтирования общей папки состояния: `/mnt/KlFocStateShare`.

   b. Введите локальный путь к точке монтирования общей папки данных: `/mnt/KlFocDataShare_klfoc`.

   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. Введите FQDN или DNS-имя вторичного сетевого адаптера либо FQDN или DNS-имя внешнего балансировщика нагрузки.

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

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

- Если число управляемых устройств составляет от 1 до 100, введите 1.
- Если число управляемых устройств составляет от 101 до 1000, введите 2.
- Если число управляемых устройств составляет более 1000, введите 3.

Этот параметр используется для автоматического определения случайной задержки запуска задач в целях оптимизации нагрузки на сеть. В списке ниже показан интервал, в пределах которого рассчитывается эта задержка:

- От 1 до 100 управляемых устройств, значение 1. Без задержки.
- От 101 до 1000 управляемых устройств, значение 2. Задержка 5 минут.
- Более 1000 управляемых устройств, значение 3. Задержка 10 минут.

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

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

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

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

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

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

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

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

n. Введите имя базы данных.

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

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

q. Введите FQDN или DNS-имя сервера IAM.

Укажите значение, которое вы указали на шаге 7e.

r. Введите имя учетной записи для запуска службы IAM. Учетная запись должна быть членом указанной группы безопасности. По умолчанию используется учетная запись ksciam.

s. Выберите СУБД, которую вы установили для работы со службой IAM:

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

t. Введите адрес СУБД IAM, который будет использоваться службой IAM.

u. Введите номер порта СУБД IAM. Этот порт используется для связи со службой IAM. По умолчанию используются следующие порты:

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

v. Введите имя базы данных IAM, которое будет использоваться службой IAM. Имя базы данных, используемой службой IAM, должно отличаться от имени базы данных, используемой Сервером администрирования.

w. Введите имя учетной записи базы данных, которая используется для доступа к базе данных IAM.

x. Введите пароль учетной записи базы данных, которая используется для доступа к базе данных IAM.

8. Подождите, пока службы добавятся и запустятся автоматически:

- klfocsvc_klfoc
- kladminserver_klfoc
- klwebsrv_klfoc
- klactprx_klfoc
- klnagent_klfoc
- kliam_klfoc

9. Создайте учетную запись, которая будет выполнять роль администратора Сервера администрирования. Введите имя пользователя и пароль. Пароль пользователя не может содержать менее 8 или более 256 символов.

Если вы пропустите этот шаг, вы можете создать учетную запись позже, выполнив команду:

```
/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <пароль>
```

Пользователь добавлен, и Kaspersky Security Center Linux установлен на первичном узле.

Установка на вторичном (пассивном) узле

Чтобы установить Kaspersky Security Center Linux на вторичный узел:

1. Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center Linux, работает один из поддерживаемых дистрибутивов Linux.

2. Запустите установку Kaspersky Security Center Linux. В зависимости от вашего дистрибутива Linux выполните одну из следующих команд:

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

3. Запустите настройку Kaspersky Security Center Linux:

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

4. 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 Linux, вам нужно 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) в соответствии с Политикой конфиденциальности. Введите `n`, если вы не принимаете условия Политики конфиденциальности. Чтобы использовать Kaspersky Security Center Linux, вам нужно принять условия Политики конфиденциальности.

5. Выберите **Вторичный узел кластера** как режим установки Сервера администрирования.

6. При появлении запроса введите локальный путь к точке монтирования общей папки состояния: `/mnt/KlFocStateShare`.

Приложение Kaspersky Security Center Linux установлено на вторичном узле.

Проверка служб

Используйте следующую команду, чтобы убедиться, что служба управления отказоустойчивым кластером находится в статусе `Active: active (running)`:

```
systemctl status klfocsvc_klfoc
```

Используйте следующие команды, чтобы убедиться, что другие службы отказоустойчивого кластера находятся в статусе `Active: inactive (dead)`:

- `systemctl status klnagent_klfoc`
- `systemctl status kladminserver_klfoc`
- `systemctl status klactprx_klfoc`

- `systemctl status klwebsrv_klfoc`
- `systemctl status kliam_klfoc`

Теперь вы можете протестировать отказоустойчивый кластер Kaspersky Security Center Linux, чтобы убедиться, что вы корректно его настроили и кластер работает правильно.

Запуск и остановка узлов 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:

На активном узле выполните одну из следующих команд:

- Чтобы остановить кластер: `/opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc`
- Чтобы запустить кластер: `/opt/kaspersky/ksc64/sbin/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`.

10. Чтобы убедится, активен ли текущий узел, выполните следующие команды, чтобы проверить, запущены ли службы:

    `systemctl status klnagent_klfoc.service`

    `systemctl status kladminserver_klfoc.service`

    `systemctl status klactprx_klfoc.service`

    `systemctl status klwebsrv_klfoc.service`

    `systemctl status kliam_klfoc.service`

    Эти службы выполняются на активном, а не на пассивном узле.

Узел обслуживается и подключается к отказоустойчивому кластеру.

Переустановка узла отказоустойчивого кластера

Чтобы переустановить узел отказоустойчивого кластера:

1. Создайте резервную копию Сервера администрирования.
2. Переключите активный узел в режим обслуживания.
3. Если необходимо сохранить текущую операционную систему, выполните следующие действия:

   Если вы хотите заменить устройство или операционную систему, пропустите этот шаг.

   a. Чтобы остановить отказоустойчивый кластер, выполните команду:

   `klfoc -stopcluster --stp klfoc`

   b. Чтобы принудительно остановить службы отказоустойчивого кластера, выполните следующие команды:

   `sudo systemctl stop klfocsvc_klfoc`

   `systemctl status kl*klfoc*`

   c. Чтобы демонтировать директории отказоустойчивого кластера, выполните следующие команды:

   `sudo umount /mnt/KlFocDataShare_klfoc`

   `sudo umount /mnt/KlFocStateShare`

   d. Чтобы удалить Kaspersky Security Center Linux, выполните одну из следующих команд в зависимости от вашего дистрибутива Linux:

   - `sudo dpkg --remove ksc64`

   Или

   - `sudo yum remove ksc64`

e. Выполните все шаги из следующих инструкций для пассивного узла:

1. Подготовка узлов для отказоустойчивого кластера Kaspersky Security Center Linux.

2. Установка Kaspersky Security Center Linux на узлы отказоустойчивого кластера Kaspersky Security Center Linux.

4. Выйдите из режима обслуживания. Продолжите с шага 6 (остановка отказоустойчивого кластера) инструкции Запуск и остановка узлов кластера вручную.

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

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

Kaspersky Security Center Web Console не поддерживает установку на узлах кластера. Рекомендуется устанавливать Kaspersky Security Center Web Console на отдельный сервер.

Чтобы установить Kaspersky Security Center 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 Web Console.

2. На шаге 3 в файле ответов, укажите параметр установки `trusted`, разрешающий Kaspersky Security Center Web Console подключаться к отказоустойчивому кластеру Kaspersky Security Center Linux.

   Компоненты параметра установки trusted

   Если вы подключаетесь к отказоустойчивому кластеру Kaspersky Security Center Linux с использованием доменной аутентификации с SSO, укажите параметры установки trusted: при подключении Kaspersky Security Center Web Console к Серверу администрирования версии 16 и выше будет использоваться доменная аутентификация с единым входом (SSO), предоставляемая Identity and Access Manager (IAM). В этом случае укажите параметры установки `trusted` следующим образом:

```
"trusted":  {
        "<Имя Сервера администрирования>": {
                "iamHost": "ksc-iam.example.com",
                "iamOAuthPort": 4444,
                "iamProxyPort": 9050,
                "iamCertPath": "<папка общих данных>/iam/main_certificate.pem",
                "iamPATPath": "<папка общих данных>/iam/initial_token.txt",
                "kscPort": 13299,
                "kscCertPath": "<папка общих данных>/1093/cert/klserver.cer"
        }
}
```

где:

- `< Имя Сервера администрирования >` – имя отказоустойчивого кластера Kaspersky Security Center Linux, которое будет отображаться в окне входа в Kaspersky Security Center Web Console.

- `iamHost` – адрес устройства, на котором установлены Сервер администрирования и IAM. Если вы создали дополнительный сетевой адаптер при подготовке узлов кластера, используйте FQDN или имя устройства адаптера в качестве адреса отказоустойчивого кластера Kaspersky Security Center Linux. В ином случае укажите FQDN или имя устройства стороннего балансировщика нагрузки, который вы используете.

  Значение `iamHost` должно совпадать с адресом IAM, указанным при установке Сервера администрирования. Для получения указанного адреса IAM выполните следующую команду на устройстве с установленным Сервером администрирования:

  ```
  grep "iam_address:" <папка общих данных>/iam/iam_config.yaml
  ```

- `iamOAuthPort` – порт, который используется для обмена токенами аутентификации по протоколу аутентификации OpenID Connect (значение по умолчанию – 4444). Этот порт используется как для связи между Сервером Kaspersky Security Center Web Console и Сервером администрирования, так и между браузером (используется с Kaspersky Security Center Web Console) и Сервером администрирования.

- `iamProxyPort` – порт, который используется для подключения Сервера Kaspersky Security Center Web Console к Серверу администрирования (значение по умолчанию – 9050).

- `iamCertPath` – это путь к IAM-сертификату. IAM-сертификат создается автоматически при первом запуске Сервера администрирования. Сертификат хранится на устройстве, на котором установлен Сервер администрирования. Путь по умолчанию к сертификату: `< общая папка данных >/iam/main_certificate.pem`. Сертификат находится в общем хранилище данных отказоустойчивого кластера Kaspersky Security Center Linux. Самоподписанный IAM-сертификат обновляется автоматически.

- `iamPATPath` – путь к токену, который используется для регистрации Kaspersky Security Center Web Console в качестве OAuth-клиента в IAM. Этот файл создается автоматически при первом запуске Сервера администрирования. Токен хранится на устройстве, на котором установлен Сервер администрирования. Путь по умолчанию к токену: <общая папка данных>/iam/initial_token.txt. Токен находится в общем хранилище данных отказоустойчивого кластера Kaspersky Security Center Linux. Токен действует бессрочно и не требует ротации.

- `kscPort` – порт OpenAPI, который Kaspersky Security Center Web Console, использует для подключения к Серверу администрирования (по умолчанию 13299).

- `kscCertPath` – сертификат Сервера администрирования, находящийся в общем хранилище данных отказоустойчивого кластера Kaspersky Security Center Linux. Путь по умолчанию к файлу сертификата: `< общая папка данных >\1093\cert\klserver.cer`.

  Скопируйте файл сертификата Сервера администрирования (по пути, указанному в параметре `kscCertPath`), файл IAM-сертификата (по пути, указанному в параметре `iamCertPath`) и файл токена (по пути, указанному в параметре `iamPATPath`) из общего хранилища данных на устройство, на котором вы устанавливаете Kaspersky Security Center Web Console. Укажите локальный путь к сертификату Сервера администрирования.

Если вы подключаете Kaspersky Security Center Web Console к Серверу администрирования версии 15.4 и ниже, аутентификация будет выполняться с использованием имени и пароля доменного пользователя или внутреннего пользователя. В этом случае укажите параметры установки trusted следующим образом:

```
"trusted":  {
        "<Имя Сервера администрирования>": {
                "kscHost": "ksc.example.com",
                "kscPort": 13299,
                "kscCertPath": "<папка общих данных>/1093/cert/klserver.cer"
        }
}
```

где:

- `<Имя Сервера администрирования>` – имя отказоустойчивого кластера Kaspersky Security Center Linux, которое будет отображаться в окне входа в Kaspersky Security Center Web Console.
- `kscHost` – это адрес Сервера администрирования (FQDN или имя устройства). Если вы создали дополнительный сетевой адаптер при подготовке узлов кластера, используйте адрес адаптера в качестве адреса отказоустойчивого кластера Kaspersky Security Center Linux. В противном случае укажите адрес стороннего балансировщика нагрузки, который вы используете.
- `kscPort` – порт OpenAPI, который Kaspersky Security Center Web Console, использует для подключения к Серверу администрирования (по умолчанию 13299).
- `kscCertPath` – сертификат Сервера администрирования, находящийся в общем хранилище данных отказоустойчивого кластера Kaspersky Security Center Linux. Путь по умолчанию к файлу сертификата: `<общая папка данных>\1093\cert\klserver.cer`. Скопируйте файл сертификата из общего хранилища данных на устройство, на котором вы устанавливаете Kaspersky Security Center Web Console. Укажите локальный путь к сертификату Сервера администрирования.

3. Продолжите стандартную установку Kaspersky Security Center Web Console.

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

Георазпределенный отказоустойчивый кластер Kaspersky Security Center Linux

В этом разделе содержится общая информация о георазпределенном отказоустойчивом кластере Kaspersky Security Center Linux, а также инструкции по подготовке и развертыванию георазпределенного отказоустойчивого кластера в вашей сети для следующих конфигураций:

- Узлы кластера под управлением Ubuntu с СУБД PostgreSQL.
- Узлы кластера под управлением SberLinux с СУБД Platform V Pangolin.

Георазпределенный кластер под управлением Ubuntu с СУБД PostgreSQL

Следуя этому сценарию, вы можете подготовить свою инфраструктуру и развернуть георазпределенный отказоустойчивый кластер Kaspersky Security Center Linux.

Предварительные требования

- Разверните высокодоступный DNS-балансировщик с проверкой работоспособности.
- Убедитесь, что активный и пассивный узлы кластера – это два устройства с одинаковой конфигурацией оборудования и программного обеспечения.
  - Аппаратные требования:
    - Процессор – 16 ядер, 2500 МГц.
    - Оперативная память – 32 ГБ.
    - Дисковое пространство – 500 ГБ с 300 IOPS или выше.
    - Контроллер сетевого интерфейса – 1 Гбит/сек.
  - Программные требования:
    - Операционная система: Ubuntu Server 24.04 LTS (Noble Numbat) 64-разрядная.
    - СУБД: PostgreSQL 17 64-разрядная.

Этапы

Отказоустойчивый кластер Kaspersky Security Center Linux, развернутый в рамках одного центра обработки данных, не может быть обновлен до геораспределенного отказоустойчивого кластера.

Развертывание геораспределенного отказоустойчивого кластера Kaspersky Security Center Linux состоит из следующих этапов:

1. **Подготовка файловой системы узлов отказоустойчивого кластера**

   Подготовьте файловую систему на обоих узлах кластера. Подготовка включает создание логических томов LVM и настройку директорий в качестве точек монтирования.

2. **Настройка реплицированной файловой системы кластера**

   Установите утилиты DRBD и настройте ресурсы DRBD для репликации данных между узлами отказоустойчивого кластера. После этого создайте реплицированную файловую систему на активном узле кластера.

3. **Установка и настройка Corosync и Pacemaker на узлах отказоустойчивого кластера**

   Установите Corosync и Pacemaker, чтобы обеспечить связь с кластером и управление ресурсами для обеспечения высокой доступности.

4. **Установка и настройка СУБД PostgreSQL**

   Установите и настройте PostgreSQL на узлах кластера.

5. **Установка Kaspersky Security Center Linux на узлы отказоустойчивого кластера**

   Установите Kaspersky Security Center Linux на узлы кластера и настройте шифрование между узлами кластера.

6 Установка Kaspersky Security Center Web Console на узлы отказоустойчивого кластера

Установите Kaspersky Security Center Web Console на оба узла отказоустойчивого кластера, чтобы обеспечить высокую доступность.

Подготовка файловой системы узлов кластера

На первом этапе подготовки к развертыванию георасределенного отказоустойчивого кластера Kaspersky Security Center Linux необходимо настроить файловую систему на обоих узлах кластера. Подготовка включает создание логических томов LVM и настройку директорий в качестве точек монтирования. Выполните описанную ниже процедуру на обоих узлах кластера.

Чтобы подготовить файловую систему узлов кластера:

1. Создайте логический том LVM для данных Сервера администрирования и базы данных:

   ```
   lvcreate -L <volume size> -n klfocdata <volume group name>
   ```

   Создайте отдельный логический том LVM для хранения файла ответов:

   ```
   lvcreate -L <volume size> -n klfocstate <volume group name>
   ```

   где:

   - `volume group name` – это имя группы томов, используемое LVM.
   - `klfocdata` и `klfocstate` – это логические имена томов. Эти логические тома создаются внутри группы томов.

     Рекомендуется использовать эти имена томов для обеспечения последовательности, хотя при необходимости вы можете указать другие имена.
   - `volume size` – размер тома. Рекомендуется выделить не менее 500 ГБ для данных Сервера администрирования и базы данных. Том для хранения файла ответов требует небольшого количества места.

2. Создайте директории, которые будут использоваться в качестве точек монтирования для логических томов.

   - Для данных Сервера администрирования и базы данных:

     ```
     mkdir -p /mnt/KlFocDataShare_klfoc
     ```

   - Для файла ответов:

     ```
     mkdir -p /mnt/KlFocStateShare_klfoc
     ```

Рекомендуется использовать директории `/mnt/KlFocDataShare_klfoc` и `/mnt/KlFocStateShare_klfoc` для единообразия, хотя при необходимости вы можете указать другие названия.

Файловая система узлов кластера подготовлена. После этого вам нужно настроить реплицированную файловую систему кластера.

Настройка реплицированной файловой системы кластера

Установка и настройка DRBD

DRBD (Distributed Replicated Block Device) – это программное обеспечение сторонних производителей, используемое для репликации данных (в частности, для томов данных и точек монтирования, подготовленных на предыдущем шаге).

После подготовки файловой системы узлов кластера нужно установить утилиты DRBD и настроить ресурсы DRBD для репликации данных между узлами кластера. Выполните описанную ниже процедуру на обоих узлах кластера.

Чтобы установить и настроить DRBD на узлах кластера:

1. Установите утилиты DRBD:

   ```
   apt update
   apt install -y drbd-utils
   ```

   Рекомендуется использовать DRBD версии 9.2.6 или выше, поскольку она обеспечивает встроенное шифрование трафика.

   Трафик DRBD также можно зашифровать с помощью собственного VPN-решения.

2. Создайте конфигурационные файлы ресурсов DRBD для каждого логического тома, созданного во время подготовки файловой системы (`klfocdata` и `klfocstate`).

   Все конфигурационные файлы должны быть помещены в `/etc/drbd.d/`.

   - Ресурс `klfocdata` (данные Сервера администрирования и база данных).

     Используйте асинхронную репликацию (протокол A) для ресурса klfocdata. Настройте все остальные параметры в соответствии с вашим окружением.

     Пример конфигурационного файла:

     ```
     resource klfocdata {
         protocol A;

         net {
             after-sb-0pri    discard-least-changes;
             after-sb-1pri    call-pri-lost-after-sb;
             after-sb-2pri    call-pri-lost-after-sb;
         }

         syncer {
             rate 110M;
         }

         # Hostname of the active node
         on db1 {
             device    /dev/drbd0;
             disk      /dev/<volume group name>/klfocdata;
             address   <disk IP address>;
             meta-disk internal;
         }

         # Hostname of the passive node
         on db2 {
             device    /dev/drbd0;
             disk      /dev/<volume group name>/klfocdata;
             address   <disk IP address>;
             meta-disk internal;
         }
     }
     ```

   - Ресурс `klfocstate` (файл ответов).

Используйте синхронную репликацию (протокол C) для создания ресурса klfocstate. Настройте все остальные параметры в соответствии с вашим окружением.

Пример конфигурационного файла:

```
resource klfocstate {
    protocol C;

    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }

    syncer {
        rate 110M;
    }

    # Hostname of the active node
    on db1 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }

    # Hostname of the passive node
    on db2 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

3. Инициализируйте метаданные DRBD для обоих ресурсов:

```
drbdadm create-md klfocdata
drbdadm create-md klfocstate
```

4. Запустите DRBD на всех настроенных ресурсах:

```
drbdadm up all
```

Приложение DRBD будет установлено и настроено на обоих узлах кластера.

Создание реплицированной файловой системы на активном узле кластера

После установки и настройки DRBD на обоих узлах кластера создайте реплицированную файловую систему на активном узле кластера. Выполните описанную ниже процедуру на активном узле кластера.

Чтобы создать реплицированную файловую систему на активном узле кластера:

1. Преобразуйте оба ресурса DRBD в основную роль:

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. Отформатируйте устройства DRBD, чтобы подготовить реплицированные тома для использования на узлах кластера:

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. Настройте параметры файловой системы:

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. Смонтируйте устройства DRBD к ранее созданным директориям:

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

Если установлена служба multipathd, она должна быть настроена на игнорирование устройств `/dev/drbd*` на обоих узлах кластера.

5. Проверьте статус репликации:

```
drbdadm status
```

Результат правильной конфигурации файловой системы:

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate

klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

Реплицированная файловая система на активном узле кластера будет настроена. После этого нужно установить и настроить Corosync и Pacemaker на узлах кластера.

Установка и настройка Corosync и Pacemaker на узлах кластера

Corosync и Pacemaker обеспечивают связь и управление ресурсами кластера для обеспечения высокой доступности. Они обеспечивают автоматическое перемещение служб на работоспособный узел в случае сбоя, сводя к минимуму время простоя.

Чтобы установить и настроить Corosync и Pacemaker на узлах кластера:

1. На обоих узлах кластера установите необходимые пакеты:

```
sudo apt install pacemaker -y
sudo apt install crmsh -y
sudo apt install resource-agent-extra -y
```

2. Настройте Corosync и Pacemaker на обоих узлах кластера согласно официальной документации. Это включает в себя включение автоматического запуска, генерацию и распространение ключа аутентификации и настройку прав доступа для файла authkey.

   Чтобы убедиться в правильности параметров, выполните следующую команду на одном из узлов кластера:

   ```
   crm status
   ```

   Ожидаемые выходные данные должны показать статус кластера и список всех активных узлов, подтверждающий, что Corosync работает правильно и узлы обмениваются данными.

3. На обоих узлах кластера настройте основные параметры кластера Pacemaker:

   ```
   crm configure property stonith-enabled="false"
   crm configure property symmetric-cluster="false"
   crm configure rsc_defaults resource-stickiness="110"
   crm configure rsc_defaults migration-threshold=3
   crm configure property no-quorum-policy=ignore
   ```

4. На обоих узлах кластера выключите запуск скриптов, которыми будет управлять Corosync:

   ```
   systemctl disable drbd.service
   ```

5. На одном из узлов кластера создайте ресурсы на основе DRBD в Pacemaker.

   - Ресурс DRBD для klfocdata

     a. Создайте ресурс кластера для тома DRBD `klfocdata`, что позволит кластеру автоматически управлять своим состоянием и отслеживать его работоспособность:

     ```
     crm configure primitive drbd_klfocdata ocf:linbit:drbd params drbd_resource="klfocdata" \
     op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
     timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
     ```

     b. Создаете ресурс управляемый кластером `ms_drbd_klfocdata` на основе созданного ресурса `drbd_klfocdata`:

     ```
     crm configure ms ms_drbd_klfocdata drbd_klfocdata meta master-max="1" master-node-max="1" \
     clone-max="2" clone-node-max="1" notify="true"
     ```

     c. Создать точку монтирования для тома DRBD `fs_klfocdata`, указав устройство, целевую директорию, тип файловой системы и параметры монтирования:

     ```
     crm configure primitive fs_klfocdata ocf:heartbeat:Filesystem params device="/dev/drbd0" \
     directory="/mnt/KlFocDataShare_klfoc" fstype="ext4" options="data=journal"
     ```

- Ресурс DRBD для klfocstate

a. Создайте ресурс кластера для тома DRBD `klfocstate`, что позволит кластеру автоматически управлять своим состоянием и отслеживать его работоспособность:

```
crm configure primitive drbd_klfocstate ocf:linbit:drbd params drbd_resource="klfocstate" \
op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
```

b. Создайте ресурс, управляемый кластером ms_drbd_klfocstate, на основе созданного ресурса `drbd_klfocstate`:

```
crm configure ms ms_drbd_klfocstate drbd_klfocstate meta master-max="1" master-node-max="1" \
clone-max="2" clone-node-max="1" notify="true"
```

c. Создайте точку монтирования для тома DRBD `fs_klfocstate`, указав устройство, целевую директорию, тип файловой системы и параметры монтирования:

```
crm configure primitive fs_klfocstate ocf:heartbeat:Filesystem params device="/dev/drbd2" \
directory="/mnt/KlFocStateShare_klfoc" fstype="ext4" options="noatime"
```

6. Определите порядок монтирования ресурсов, там где DRBD находятся в состоянии Primary. Назовите этот ресурс `cluster_resources`:

```
crm configure colocation cluster_resources inf: fs_klfocdata ms_drbd_klfocdata:Master ms_drbd_klfocstate:Master
```

7. Определите группу ресурсов и служб `group_klfoc`:

```
crm configure group group_klfoc fs_klfocdata fs_klfocstate
```

8. Настройте запуск группы ресурсов `group_klfoc` после соответствующих DRBD ресурсов. Назовите это правило `all_after_drbd`:

```
crm configure order all_after_drbd inf: ms_drbd_klfocdata:promote group_klfoc:start
```

9. Задайте предпочтение для запуска первичных и вторичных ресурсов: приоритет 100 для `node1` и 50 для `node2`:

```
crm configure location loc_klfocdata_one ms_drbd_klfocdata 100: db1 # hostname of the first cluster node
crm configure location loc_klfocdata_two ms_drbd_klfocdata 50: db2 # hostname of the second cluster node
crm configure location loc_klfocstate_one ms_drbd_klfocstate 100: db1 # hostname of the first cluster node
crm configure location loc_klfocstate_two ms_drbd_klfocstate 50: db2 # hostname of the second cluster node
crm configure location loc_group_one group_klfoc 100: db1 # hostname of the first cluster node
crm configure location loc_group_two group_klfoc 50: db2 # hostname of the second cluster node
```

10. На обоих узлах кластера выключите автоматический запуск службы DRBD:

```
systemctl disable drbd.service
```

Corosync и Pacemaker будут установлены и настроены на узлах кластера. После этого нужно установить СУБД и создать базу данных Сервера администрирования и базу данных IAM.

Установка и настройка СУБД PostgreSQL

После установки и настройки Corosync и Pacemaker на узлах кластера нужно установить СУБД на обоих узлах кластера.

Чтобы установить и настроить СУБД:

1. На обоих узлах кластера установите PostgreSQL 17 x64 или выше.

   Подробнее о том как установить PostgreSQL, см. в соответствующей документации.

2. Убедитесь, что на узлах кластера с установленной СУБД нет учетных записей пользователей СУБД со следующими именами:

   - client
   - iam
   - ksc
   - locker
   - pat
   - scope
   - voltron

3. На обоих узлах кластера остановите СУБД и выключите автоматический запуск службы СУБД:

   ```
   sudo systemctl stop postgresql
   sudo systemctl disable postgresql
   ```

4. На активном узле кластера скопируйте директорию СУБД в директорию `/mnt/KlFocDataShare_klfoc/dbms`:

   ```
   rsync -av /var/lib/postgresql/17/main/ /mnt/KlFocDataShare_klfoc/dbms
   mv /var/lib/postgresql/17/main /var/lib/postgresql/17/main.bk
   ```

5. На активном узле кластера скопируйте конфигурационные файлы PostgreSQL в директорию `/mnt/KlFocDataShare_klfoc/dbms`:

   ```
   sudo cp /etc/postgresql/17/main/pg_hba.conf /mnt/KlFocDataShare_klfoc/dbms
   sudo cp /etc/postgresql/17/main/pg_ident.conf /mnt/KlFocDataShare_klfoc/dbms
   ```

6. На обоих узлах кластера откройте конфигурационный файл `/etc/postgresql/17/main/postgresql.conf` и укажите директорию `/mnt/KlFocDataShare_klfoc/dbms` в качестве директории данных базы.

   Также укажите пути к конфигурационным файлам (`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf` и `/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`) и удалите параметр `include_dir`:

   ```
   data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
   hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
   ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
   listen_addresses = '*'
   ```

7. В конфигурационном файле `/etc/postgresql/17/main/postgresql.conf` настройте конфигурацию СУБД в соответствии с требованиями Kaspersky Security Center Linux.

8. Создайте и настройте учетные записи для работы с PostgreSQL.

9. Создайте ресурс службы PostgreSQL:

   ```
   crm configure primitive klfocsvc_dbms ocf:heartbeat:pgsql \
   params pgctl="/usr/lib/postgresql/17/bin/pg_ctl" \
   psql="/usr/bin/psql" \
   pgdata="/mnt/KlFocDataShare_klfoc/dbms" \
   config="/etc/postgresql/17/main/postgresql.conf" \
   socketdir="/var/run/postgresql" \
   op start timeout=60s \
   op stop timeout=60s \
   op monitor interval=30s timeout=60s
   ```

10. Добавьте ресурс PostgreSQL в группу кластеров `group_klfoc`:

    ```
    crm configure edit group_klfoc
    ```

11. Добавить имя ресурса PostgreSQL `klfocsvc_dbms` в конец списка, например:

    ```
    group group_klfoc {
    ...
    klfocsvc_dbms
    }
    ```

12. На активном узле кластера сервера СУБД создайте базу данных для IAM. Имя базы данных должно отличаться от имени базы данных, которую вы установили для работы с Kaspersky Security Center Linux. Сервер администрирования не удаляет базу данных IAM автоматически при деинсталляции или переносе Сервера на другое устройство, вам нужно удалить базу данных вручную:

    ```
    sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
    ```

СУБД будет установлена и настроена. База данных Сервера администрирования и база данных IAM созданы. После этого вам нужно установить Kaspersky Security Center Linux на узлы кластера.

Установка Kaspersky Security Center Linux на узлы геораспределенного отказоустойчивого кластера

Kaspersky Security Center Linux устанавливается на узлы геораспределенного отказоустойчивого кластера с использованием файла ответов в тихом режиме, то есть без участия пользователя. Файл ответов содержит настраиваемый набор параметров установки: переменные и соответствующие им значения.

Предварительные требования:

- Выполните все подготовительные шаги:
  - Подготовка файловой системы узлов кластера
  - Настройка реплицированной файловой системы кластера
  - Установка и настройка Corosync и Pacemaker на узлах кластера
  - Установка и настройка СУБД PostgreSQL
- Убедитесь, что узлы кластера работают под управлением Ubuntu Server 24.04 LTS (Noble Numbat) x64.
- Загрузите установочный файл `ksc64_[version_number]_amd64.deb` с сайта "Лаборатории Касперского".

Установка на активный узел

Чтобы установить Kaspersky Security Center Linux на активном узле в тихом режиме:

1. Прочитайте Лицензионное соглашение. Следуйте шагам ниже, только если вы понимаете и принимаете условия Лицензионного соглашения.
2. Создайте группу `kladmins` и непривилегированные учетные записи `ksc` и `ksciam`, которые должны быть членами 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
   adduser ksciam
   gpasswd -a ksciam kladmins
   usermod -g kladmins ksciam
   ```

3. В директории `/mnt/KlFocDataShare_klfoc/` создайте директорию для файлов Kaspersky Security Center Linux:

   ```
   mkdir /mnt/KlFocDataShare_klfoc/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.

   В списке параметров, используемых для установки Kaspersky Security Center Linux в тихом режиме, укажите следующие параметры, необходимые для развертывания геораспределенного кластера:

   - `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

     Установите значение `2`, чтобы развернуть геораспределенный кластер.

   - `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>` и `KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

     DNS-балансировщик с проверкой работоспособности должен быть уже развернут. Значения этих параметров должны быть одинаковыми и соответствовать FQDN DNS-балансировщика.

5. Задайте для переменной среды `KLAUTOANSWERS` в среде root или пользователя значение, содержащее полное имя файла ответов, включая путь, например, с помощью следующей команды:

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

6. Запустите установку Kaspersky Security Center Linux в тихом режиме, выполнив следующие команды:

   - В корневой среде:

     ```
     apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
     ```

   - В пользовательской среде:

     ```
     sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
     ```

7. Выключите автоматический запуск службы klfocsvc_klfoc.service:

   ```
   systemctl disable klfocsvc_klfoc.service
   ```

8. После установки Kaspersky Security Center Linux остановите активный узел кластера.

9. Переместите все ресурсы кластера на пассивный узел.

   Вы можете использовать команду `crm node standby` (и вернуть их с помощью команды `crm node online`).

Установка на пассивном узле

Чтобы установить Kaspersky Security Center Linux на пассивном узле:

1. Запустите установку Kaspersky Security Center Linux:

   ```
   sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
   ```

2. Запустите настройку Kaspersky Security Center Linux:

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

3. 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:

   - Введите `y`, если вы понимаете и принимаете условия Лицензионного соглашения. Введите `n`, если вы не принимаете условия Лицензионного соглашения. Чтобы использовать Kaspersky Security Center Linux, вам нужно принять условия Лицензионного соглашения.

   - 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) в соответствии с Политикой конфиденциальности. Введите n, если вы не принимаете условия Политики конфиденциальности. Чтобы использовать Kaspersky Security Center Linux, вам нужно принять условия Политики конфиденциальности.

4. Выберите пассивный узел кластера в качестве режима установки Сервера администрирования.

5. При появлении запроса введите локальный путь к точке монтирования общей папки состояния: `/mnt/KlFocStateShare_klfoc`.

6. Выключите автоматический запуск службы klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

7. Создайте ресурс службы `klfocsvc_klfoc`:

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. Добавьте ресурс `klfocsvc_klfoc` в группу `group_klfoc`:

```
crm configure edit group_klfoc
```

9. Добавьте параметр `klfocsvc_klfoc` в конец группы, например:

```
group group_klfoc {
...
klfocsvc_klfoc
}
```

10. Убедитесь, что все ресурсы на активном узле находятся в запущенном состоянии.

```
crm status
```

Настройка шифрования между узлами кластера

Чтобы настроить шифрование между узлами кластера,

Если вы установили DRBD версии 9.2.6 или выше во время настройки реплицированной файловой системы кластера, настройте шифрование между узлами кластера в соответствии с официальной документацией DRBD.

Также вы можете настроить шифрование трафика между узлами кластера, используя собственное VPN-решение.

Георасределенный отказоустойчивый кластер Kaspersky Security Center Linux установлен. После этого вам нужно установить Kaspersky Security Center Web Console на оба узла кластера.

Георасределенный кластер под управлением SberLinux с СУБД Platform V Pangolin

Следуя этому сценарию, вы можете подготовить свою инфраструктуру и развернуть георасределенный отказоустойчивый кластер Kaspersky Security Center Linux.

Предварительные требования

- Разверните высокодоступный DNS-балансировщик с проверкой работоспособности.
- Убедитесь, что активный и пассивный узлы кластера – это два устройства с одинаковой конфигурацией оборудования и программного обеспечения.
  - Аппаратные требования:
    - Процессор – 16 ядер, 2500 МГц.
    - Оперативная память – 32 ГБ.
    - Дисковое пространство – 500 ГБ с 300 IOPS или выше.
    - Контроллер сетевого интерфейса – 1 Гбит/сек.
  - Программные требования:
    - Операционная система: Platform V SberLinux OS Server (SLO) 9.5.1 64-разрядная.
    - СУБД: Platform V Pangolin 6.5.1 64-разрядная.

Этапы

Отказоустойчивый кластер Kaspersky Security Center Linux, развернутый в рамках одного центра обработки данных, не может быть обновлен до георасределенного отказоустойчивого кластера.

Развертывание георасределенного отказоустойчивого кластера Kaspersky Security Center Linux состоит из следующих этапов:

1. **Подготовка файловой системы узлов отказоустойчивого кластера**

   Подготовьте файловую систему на обоих узлах кластера. Подготовка включает создание логических томов LVM и настройку директорий в качестве точек монтирования.

2. **Настройка реплицированной файловой системы кластера**

   Установите утилиты DRBD и настройте ресурсы DRBD для репликации данных между узлами отказоустойчивого кластера. После этого создайте реплицированную файловую систему на активном узле кластера.

3. **Установка и настройка Corosync и Pacemaker на узлах отказоустойчивого кластера**

   Установите Corosync и Pacemaker, чтобы обеспечить связь с кластером и управление ресурсами для обеспечения высокой доступности.

4. **Установка и настройка СУБД Platform V Pangolin**

   Установите и настройте Platform V Pangolin на узлах кластера.

5. **Установка Kaspersky Security Center Linux на узлы отказоустойчивого кластера**

   Установите Kaspersky Security Center Linux на узлы кластера и настройте шифрование между узлами кластера.

6. **Установка Kaspersky Security Center Web Console на узлы отказоустойчивого кластера**

   Установите Kaspersky Security Center Web Console на оба узла отказоустойчивого кластера, чтобы обеспечить высокую доступность.

Подготовка файловой системы узлов кластера

На первом этапе подготовки к развертыванию георасределенного отказоустойчивого кластера Kaspersky Security Center Linux необходимо настроить файловую систему на обоих узлах кластера. Подготовка включает создание логических томов LVM и настройку директорий в качестве точек монтирования. Выполните описанную ниже процедуру на обоих узлах кластера.

Чтобы подготовить файловую систему узлов кластера:

1. Создайте логический том LVM для данных Сервера администрирования и базы данных:

   ```
   lvcreate -L <volume size> -n klfocdata <volume group name>
   ```

   Создайте отдельный логический том LVM для хранения файла ответов:

   ```
   lvcreate -L <volume size> -n klfocstate <volume group name>
   ```

   где:

   - `volume group name` – это имя группы томов, используемое LVM.
   - `klfocdata` и `klfocstate` – это логические имена томов. Эти логические тома создаются внутри группы томов.

     Рекомендуется использовать эти имена томов для обеспечения последовательности, хотя при необходимости вы можете указать другие имена.

   - `volume size` – размер тома. Рекомендуется выделить не менее 500 ГБ для данных Сервера администрирования и базы данных. Том для хранения файла ответов требует небольшого количества места.

2. Создайте директории, которые будут использоваться в качестве точек монтирования для логических томов.

   - Для данных Сервера администрирования и базы данных:

     ```
     mkdir -p /mnt/KlFocDataShare_klfoc
     ```

- Для файла ответов:

```
mkdir -p /mnt/KlFocStateShare_klfoc
```

Рекомендуется использовать директории `/mnt/KlFocDataShare_klfoc` и `/mnt/KlFocStateShare_klfoc` для единообразия, хотя при необходимости вы можете указать другие названия.

Файловая система узлов кластера подготовлена. После этого вам нужно настроить реплицированную файловую систему кластера.

Настройка реплицированной файловой системы кластера

Установка и настройка DRBD

DRBD (Distributed Replicated Block Device) – это программное обеспечение сторонних производителей, используемое для репликации данных (в частности, для томов данных и точек монтирования, подготовленных на предыдущем шаге).

После подготовки файловой системы узлов кластера нужно установить утилиты DRBD и настроить ресурсы DRBD для репликации данных между узлами кластера. Выполните описанную ниже процедуру на обоих узлах кластера.

Чтобы установить и настроить DRBD на узлах кластера:

1. Установите утилиты DRBD следующим образом:

   a. Включите хранилища EPEL и ELRepo на обоих узлах:

   ```
   dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   dnf install https://www.elrepo.org/elrepo-release-9.el9.elrepo.noarch.rpm
   ```

   b. Выведите все доступные версии пакета kmod-drbd9x и отфильтруйте список пакетов, созданные для платформы el9_6 (например, Platform V SberLinux OS Server (SLO) 9.6):

   ```
   dnf search --showduplicates kmod-drbd9x | grep el9_6
   ```

   c. Установите последнюю доступную версию из списка на обоих узлах. Пример для Platform V SberLinux OS Server (SLO) 9.6:

   ```
   dnf install kmod-drbd9x-9.2.14-1.el9_6.elrepo.x86_64
   dnf install drbd drbd-utils drbd-udev drbd-pacemaker drbd-selinux
   modprobe drbd
   ```

   Если в будущем появится более новая версия, замените строку с версией соответствующим образом.

   Рекомендуется использовать DRBD версии 9.2.6 или выше, поскольку она обеспечивает встроенное шифрование трафика.

   Трафик DRBD также можно зашифровать с помощью собственного VPN-решения.

2. Создайте конфигурационные файлы ресурсов DRBD для каждого логического тома, созданного во время подготовки файловой системы (`klfocdata` и `klfocstate`).

Все конфигурационные файлы должны быть помещены в `/etc/drbd.d/`.

- Ресурс `klfocdata` (данные Сервера администрирования и база данных).

  Используйте асинхронную репликацию (протокол A) для ресурса klfocdata. Настройте все остальные параметры в соответствии с вашим окружением.

  Пример конфигурационного файла:

```
resource klfocdata {
    protocol A;

    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }

    syncer {
        rate 110M;
    }

    # Hostname of the active node
    on db1 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }

    # Hostname of the passive node
    on db2 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

- Ресурс `klfocstate` (файл ответов).

  Используйте синхронную репликацию (протокол C) для создания ресурса klfocstate. Настройте все остальные параметры в соответствии с вашим окружением.

  Пример конфигурационного файла:

```
resource klfocstate {
    protocol C;

    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }

    syncer {
        rate 110M;
    }

    # Hostname of the active node
    on db1 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }

    # Hostname of the passive node
    on db2 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
```

```
    }
}
```

3. Инициализируйте метаданные DRBD для обоих ресурсов:

```
drbdadm create-md klfocdata
drbdadm create-md klfocstate
```

4. Запустите DRBD на всех настроенных ресурсах:

```
drbdadm up all
```

Приложение DRBD будет установлено и настроено на обоих узлах кластера.

Создание реплицированной файловой системы на активном узле кластера

После установки и настройки DRBD на обоих узлах кластера создайте реплицированную файловую систему на активном узле кластера. Выполните описанную ниже процедуру на активном узле кластера.

Чтобы создать реплицированную файловую систему на активном узле кластера:

1. Преобразуйте оба ресурса DRBD в основную роль:

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. Отформатируйте устройства DRBD, чтобы подготовить реплицированные тома для использования на узлах кластера:

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. Настройте параметры файловой системы:

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. Смонтируйте устройства DRBD к ранее созданным директориям:

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

Если установлена служба multipathd, она должна быть настроена на игнорирование устройств `/dev/drbd*` на обоих узлах кластера.

5. Проверьте статус репликации:

```
drbdadm status
```

Результат правильной конфигурации файловой системы:

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate

klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

Реплицированная файловая система на активном узле кластера будет настроена. После этого нужно установить и настроить Corosync и Pacemaker на узлах кластера.

Установка и настройка Corosync и Pacemaker на узлах кластера

Corosync и Pacemaker обеспечивают связь и управление ресурсами кластера для обеспечения высокой доступности. Они обеспечивают автоматическое перемещение служб на работоспособный узел в случае сбоя, сводя к минимуму время простоя.

Чтобы установить и настроить Corosync и Pacemaker на узлах кластера:

1. На обоих узлах кластера установите необходимые пакеты:

```
dnf install pcs
dnf install drbd-pacemaker
```

2. Настройте Corosync и Pacemaker на обоих узлах кластера согласно официальной документации. Это включает в себя включение автоматического запуска, генерацию и распространение ключа аутентификации и настройку прав доступа для файла authkey.

   Чтобы убедиться в правильности параметров, выполните следующую команду на одном из узлов кластера:

```
pcs status
```

   Ожидаемые выходные данные должны показать статус кластера и список всех активных узлов, подтверждающий, что Corosync работает правильно и узлы обмениваются данными.

3. На обоих узлах кластера настройте основные параметры кластера Pacemaker:

```
pcs property set stonith-enabled=false
pcs property set symmetric-cluster=false
pcs resource defaults resource-stickiness=110
pcs resource defaults migration-threshold=3
pcs property set no-quorum-policy=ignore
```

4. На обоих узлах кластера выключите запуск скриптов, которыми будет управлять Corosync:

```
systemctl disable drbd.service
```

5. На одном из узлов кластера создайте ресурсы на основе DRBD в Pacemaker.

- Ресурс DRBD для klfocdata

  a. Создайте ресурс кластера для тома DRBD `klfocdata`, что позволит кластеру автоматически управлять своим состоянием и отслеживать его работоспособность:

  ```
  pcs resource create drbd_klfocdata ocf:linbit:drbd \
  drbd_resource="klfocdata" \
  op monitor interval=60s \
  op start interval=0 timeout=240s \
  op stop interval=0 timeout=240s \
  op monitor role=Master interval=10s \
  op monitor role=Slave interval=30s \
  ```

  b. Создаете ресурс управляемый кластером `ms_drbd_klfocdata` на основе созданного ресурса `drbd_klfocdata`:

  ```
  pcs resource clone drbd_klfocdata promotable=true
  master-max=1
  clone-max=2
  clone-node-max=1 notify=true
  ```

  c. Создать точку монтирования для тома DRBD `fs_klfocdata`, указав устройство, целевую директорию, тип файловой системы и параметры монтирования:

  ```
  pcs resource create fs_klfocdata ocf:heartbeat:Filesystem \
  device="/dev/drbd0" \
  directory="/mnt/KlFocDataShare_klfoc" \
  fstype="ext4" \
  options="data=journal"
  ```

- Ресурс DRBD для klfocstate

  a. Создайте ресурс кластера для тома DRBD `klfocstate`, что позволит кластеру автоматически управлять своим состоянием и отслеживать его работоспособность:

  ```
  pcs resource create drbd_klfocstate ocf:linbit:drbd \
  drbd_resource=klfocstate \
  op monitor interval=60s \
  op start interval=0 timeout=240s \
  op stop interval=0 timeout=240s \
  op monitor role=Promoted interval=10s \
  op monitor role=Unpromoted interval=30s \
  ```

  b. Создайте ресурс, управляемый кластером ms_drbd_klfocstate, на основе созданного ресурса `drbd_klfocstate`:

  ```
  pcs resource clone drbd_klfocstate promotable=true \
  master-max=1 \
  clone-max=2 \
  clone-node-max=1 \
  notify=true
  ```

c. Создайте точку монтирования для тома DRBD `fs_klfocstate`, указав устройство, целевую директорию, тип файловой системы и параметры монтирования:

```
pcs resource create fs_klfocstate ocf:heartbeat:Filesystem \
device="/dev/drbd2" \
directory="/mnt/KlFocStateShare_klfoc" \
fstype="ext4" \
options="noatime"
```

6. На обоих узлах кластера выключите автоматический запуск службы DRBD:

```
systemctl disable drbd.service
```

Corosync и Pacemaker будут установлены и настроены на узлах кластера. После этого нужно установить СУБД и создать базу данных Сервера администрирования и базу данных IAM.

Установка и настройка СУБД Platform V Pangolin

После установки и настройки Corosync и Pacemaker на узлах кластера нужно установить СУБД на обоих узлах кластера.

Чтобы установить и настроить СУБД:

1. На обоих узлах кластера установите Platform V Pangolin 6.5.1 x64 или выше.

   Подробнее о том, как установить выбранную СУБД Platform V Pangolin, см. в документации к этой СУБД.

2. Убедитесь, что на узлах кластера с установленной СУБД нет учетных записей пользователей СУБД со следующими именами:

   - client
   - iam
   - ksc
   - locker
   - pat
   - scope
   - voltron

3. На активном узле кластера скопируйте директорию СУБД в директорию `/mnt/KlFocDataShare_klfoc/dbms`:

```
sudo rsync -av  /pgdata/06/data/ /mnt/KlFocDataShare_klfoc/dbms
sudo mv /pgdata/06/data/ /pgdata/06/data.bk/
```

4. На обоих узлах кластера откройте конфигурационный файл `/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf` и укажите директорию `/mnt/KlFocDataShare_klfoc/dbms` в качестве директории данных базы.

   Также укажите пути к конфигурационным файлам (`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf` и `/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`) и удалите параметр `include_dir`:

   ```
   data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
   hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
   ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
   listen_addresses = '*'
   ```

5. В конфигурационном файле `/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf` настройте конфигурацию СУБД в соответствии с требованиями Kaspersky Security Center Linux.

6. Создайте и настройте учетные записи для работы с PostgreSQL.

7. Создайте ресурс службы СУБД:

   ```
   pcs resource create klfocsvc_dbms pgsql \
   pgctl="/usr/pangolin-6.5/bin/pg_ctl"  psql="/usr/bin/psql" pgdata="/mnt/KlFocDataShare_klfoc/dbms"
   config="/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf" socketdir="/tmp" \
   op start timeout=60s interval=0s \
   op stop timeout=60s interval=0s \
   op monitor interval=30s timeout=60s \
   op promote timeout=120s interval=0s \
   op demote timeout=120s interval=0s \
   meta target-role=Started
   ```

8. На обоих узлах кластера выключите автоматический запуск службы СУБД:

   ```
   sudo systemctl disable pangolin.service
   ```

9. Добавьте ресурс СУБД `klfocsvc_dbms` в группу кластеров `group_klfoc`:

   ```
   pcs resource group add group_klfoc klfocsvc_dbms
   ```

10. Добавьте имя ресурса СУБД `klfocsvc_dbms` в конце списка, например:

    ```
    group group_klfoc {
    ...
    klfocsvc_dbms
    }
    ```

11. На активном узле кластера сервера СУБД создайте базу данных для IAM. Имя базы данных должно отличаться от имени базы данных, которую вы установили для работы с Kaspersky Security Center Linux. Сервер администрирования не удаляет базу данных IAM автоматически при деинсталляции или переносе Сервера на другое устройство, вам нужно удалить базу данных вручную:

    ```
    sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
    ```

СУБД будет установлена и настроена. База данных Сервера администрирования и база данных IAM созданы. После этого вам нужно установить Kaspersky Security Center Linux на узлы кластера.

Установка Kaspersky Security Center Linux на узлы геораспределенного отказоустойчивого кластера

Kaspersky Security Center Linux устанавливается на узлы геораспределенного отказоустойчивого кластера с использованием файла ответов в тихом режиме, то есть без участия пользователя. Файл ответов содержит настраиваемый набор параметров установки: переменные и соответствующие им значения.

Предварительные требования:

- Выполните все подготовительные шаги:
  - Подготовка файловой системы узлов кластера
  - Настройка реплицированной файловой системы кластера
  - Установка и настройка Corosync и Pacemaker на узлах кластера
  - Установка и настройка СУБД Platform V Pangolin
- Убедитесь, что узлы кластера работают под управлением Platform V SberLinux OS Server (SLO) 9.5.1 x64.
- Загрузите установочный файл `ksc64_[version_number]_amd64.deb` с сайта "Лаборатории Касперского".

Установка на активный узел

Чтобы установить Kaspersky Security Center Linux на активном узле в тихом режиме:

1. Прочитайте Лицензионное соглашение. Следуйте шагам ниже, только если вы понимаете и принимаете условия Лицензионного соглашения.
2. Создайте группу `kladmins` и непривилегированные учетные записи `ksc` и `ksciam`, которые должны быть членами 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
   adduser ksciam
   gpasswd -a ksciam kladmins
   usermod -g kladmins ksciam
   ```

3. В директории `/mnt/KlFocDataShare_klfoc/` создайте директорию для файлов Kaspersky Security Center Linux:

   ```
   mkdir /mnt/KlFocDataShare_klfoc/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.

В списке параметров, используемых для установки Kaspersky Security Center Linux в тихом режиме, укажите следующие параметры, необходимые для развертывания геораспределенного кластера:

- `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

  Установите значение `2`, чтобы развернуть геораспределенный кластер.

- `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>` и `KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

  DNS-балансировщик с проверкой работоспособности должен быть уже развернут. Значения этих параметров должны быть одинаковыми и соответствовать FQDN DNS-балансировщика.

5. Задайте для переменной среды `KLAUTOANSWERS` в среде root или пользователя значение, содержащее полное имя файла ответов, включая путь, например, с помощью следующей команды:

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

6. Запустите установку Kaspersky Security Center Linux в тихом режиме, выполнив следующие команды:

   - В корневой среде:

   ```
   apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
   ```

   - В пользовательской среде:

   ```
   sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
   ```

7. Выключите автоматический запуск службы klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

8. После установки Kaspersky Security Center Linux остановите активный узел кластера.

9. Переместите все ресурсы кластера на пассивный узел.

   Вы можете использовать команду `pcs node standby` (и вернуть их с помощью команды `pcs node online`).

Установка на пассивном узле

Чтобы установить Kaspersky Security Center Linux на пассивном узле:

1. Запустите установку Kaspersky Security Center Linux:

```
sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
```

2. Запустите настройку Kaspersky Security Center Linux:

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

3. 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:

   - Введите `y`, если вы понимаете и принимаете условия Лицензионного соглашения. Введите `n`, если вы не принимаете условия Лицензионного соглашения. Чтобы использовать Kaspersky Security Center Linux, вам нужно принять условия Лицензионного соглашения.

   - 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) в соответствии с Политикой конфиденциальности. Введите n, если вы не принимаете условия Политики конфиденциальности. Чтобы использовать Kaspersky Security Center Linux, вам нужно принять условия Политики конфиденциальности.

4. Выберите пассивный узел кластера в качестве режима установки Сервера администрирования.

5. При появлении запроса введите локальный путь к точке монтирования общей папки состояния: `/mnt/KlFocStateShare_klfoc`.

6. Выключите автоматический запуск службы klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

7. Создайте ресурс службы `klfocsvc_klfoc`:

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. Добавьте ресурс `klfocsvc_klfoc` в группу `group_klfoc`:

```
pcs resource group add group_klfoc klfocsvc_klfoc
```

9. Добавьте параметр `klfocsvc_klfoc` в конец группы, например:

```
group group_klfoc {
...
klfocsvc_klfoc
}
```

10. Убедитесь, что все ресурсы на активном узле находятся в запущенном состоянии.

```
pcs status
```

Настройка шифрования между узлами кластера

Чтобы настроить шифрование между узлами кластера,

Если вы установили DRBD версии 9.2.6 или выше во время настройки реплицированной файловой системы кластера, настройте шифрование между узлами кластера в соответствии с официальной документацией DRBD.

Также вы можете настроить шифрование трафика между узлами кластера, используя собственное VPN-решение.

Георасределенный отказоустойчивый кластер Kaspersky Security Center Linux установлен. После этого вам нужно установить Kaspersky Security Center Web Console на оба узла кластера.

Установка Kaspersky Security Center Web Console на узлы георасределенного отказоустойчивого кластера

Для георасределенного развертывания отказоустойчивого кластера Kaspersky Security Center Linux должна поддерживаться высокая доступность Kaspersky Security Center Web Console. Для этого на обоих узлах кластера должно быть установлено приложение Kaspersky Security Center Web Console.

Чтобы установить Kaspersky Security Center Web Console:

1. На обоих узлах создайте учетную запись для работы с Kaspersky Security Center Web Console. Для этого выполните следующую команду под учетной записью с правами root:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>
   ```

   где пароль должен содержать не менее 8 символов.

2. На обоих узлах ознакомьтесь с Лицензионным соглашением. Если в состав дистрибутива Kaspersky Security Center Linux не входит TXT-файл с текстом Лицензионного соглашения, вы можете загрузить этот файл с сайта "Лаборатории Касперского". Если вы не согласны с условиями Лицензионного соглашения, не устанавливайте приложение.

3. На обоих узлах создайте файл ответов, который содержит параметры для подключения Kaspersky Security Center Web Console к Серверу администрирования: `/etc/ksc-web-console-setup.json`.

   Пример файла ответов с минимальным набором параметров

   Набор параметров файла ответов зависит от версии Сервера администрирования, к которому подключено приложение Kaspersky Security Center Web Console:

   - Сервер администрирования версии 16 и выше

     Пример файла ответов с минимальным набором параметров для входа на Сервер администрирования версии 16 и выше:

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
             "Administration Server v16": {
                 "iamHost": "ksc16.example.com",
                 "iamOAuthPort": 4444,
                 "iamProxyPort": 9050,
                 "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
                 "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
                 "kscPort": 13299,
                 "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
             }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

- Сервер администрирования версии 15.4 и выше

  Пример файла ответов с минимальным набором параметров для входа на Сервер администрирования версии 15.4 и ниже:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Вы можете установить Kaspersky Security Center Web Console на том же устройстве, что и Сервер администрирования, или на другом устройстве. Если приложение Kaspersky Security Center Web Console установлено на другом устройстве, адрес Kaspersky Security Center Web Console (параметр `address`) и адрес Сервера администрирования (параметр `iamHost` или `kscHost`) отличаются. Если приложение Kaspersky Security Center Web Console установлено на одном устройстве с Сервером администрирования, эти параметры имеют одинаковые значения.

Значение `iamHost` должно совпадать с адресом IAM, который вы указали при установке Сервера администрирования. Для получения указанного адреса IAM выполните следующую команду на устройстве с установленным Сервером администрирования:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Подробную информацию см. в статье Параметры установки Kaspersky Security Center Web Console.

Вы можете добавить несколько Серверов администрирования разных версий в список доверенных серверов. В этом случае Серверы могут использовать разные способы аутентификации.

Рекомендуется указывать номера портов больше 1024. Если вы хотите, чтобы приложение Kaspersky Security Center Web Console работало на портах ниже 1024, после установки убедитесь, что у вас установлена утилита setcap, а затем выполните команду:

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

Если у вас нет утилиты setcap, вы можете ее установить. **Перейдите по этой ссылке, чтобы просмотреть команды**

Для операционных систем Debian и Ubuntu выполните одну из следующих команд:

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

Для SUSE Linux Enterprise Server и Red Hat Enterprise Linux выполните команду:

- `sudo zypper install libcap-progs`

4. На обоих узлах запустите установочный файл под учетной записью с правами root.

```
sudo apt-get install ksc-web-console-<build number>.x86_64.deb
```

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

5. На одном из узлов кластера создайте ресурс Pacemaker для службы KSCWebConsole, чтобы сделать KSCWebConsole службой, управляемой Pacemaker:

```
crm configure primitive ksc_webconsole systemd:KSCWebConsole \
op monitor interval=30s timeout=60s \
op start timeout=120s \
op stop timeout=120s \
meta target-role=Stopped
```

6. На обоих узлах остановите службу KSCWebConsole и выключите ее автоматический запуск:

```
sudo systemctl stop KSCWebConsole
sudo systemctl disable KSCWebConsole
```

7. На одном из узлов кластера добавьте ресурс `ksc_webconsole` в группу `group_klfoc`:

```
crm configure edit group_klfoc
```

8. Добавьте параметр `ksc_webconsole` в конец группы после `klfocsvc_dbms`, например:

```
group group_klfoc {
...
klfocsvc_dbms
ksc_webconsole
}
```

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

Учетные записи для работы с СУБД

Для установки Сервера администрирования и IAM, а также для дальнейшей работы с ними требуются внутренние учетные записи СУБД. Эти учетные записи позволяют вам получить доступ к СУБД и требуют наличия определенных прав.

Набор необходимых прав зависит от следующих критериев:

- Тип СУБД:
  - MySQL или MariaDB.
  - Основана на PostgreSQL.

- Способ создания базы данных Сервера администрирования:
  - **Автоматически**. При установке Сервера администрирования вы можете автоматически создать базу данных Сервера администрирования (далее также база данных Сервера) с помощью приложения установки Сервера администрирования (инсталлятора).
  - **Вручную**. Можно использовать приложение стороннего производителя или скрипт для создания пустой базы данных. После этого вы можете указать эту базу данных в качестве базы данных Сервера при установке Сервера администрирования.

База данных для IAM должна быть создана вручную независимо от выбранного способа создания базы данных Сервера администрирования.

При предоставлении прав и разрешений учетным записям соблюдайте принцип наименьших привилегий. Это означает, что предоставленных прав достаточно только для выполнения требуемых действий. Не используйте стандартные учетные записи суперпользователей СУБД такие как root и postgres в качестве пользователя подключения к СУБД для Kaspersky Security Center Linux.

Не вносите вручную изменения в базу данных Сервера администрирования и базу данных IAM, включая изменение значений, удаление или добавление схем, таблиц, индексов. Любые изменения в базах данных, не выполненные самим Сервером администрирования, нарушают нормальную работу Сервера администрирования сразу или позже, например после обновления до более новой версии или при восстановлении из резервной копии. Изменение баз разрешено только в том случае, если вы получили точные инструкции от Службы технической поддержки "Лаборатории Касперского".
При деинсталляции или переносе Сервера на другое устройство, вам нужно удалить базы данных Сервера администрирования и IAM вручную.

Ниже представлена информация о правах на СУБД, которые требуется предоставить учетным записям перед установкой и запуском Сервера администрирования.

MySQL и MariaDB

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

- Схема привилегий:
  - База данных Сервера администрирования: ALL (кроме GRANT OPTION).
  - Схемы системы (mysql и sys): SELECT, SHOW VIEW.
  - Хранимая процедура sys.table_exists: EXECUTE (если вы используете MariaDB 10.5 или более раннюю версию в качестве СУБД, вам не нужно предоставлять право EXECUTE).
- Глобальные привилегии для всех схем: PROCESS, SUPER.

Подробнее о настройке прав учетной записи см. в статье Создание баз и учетных записей СУБД MySQL и MariaDB.

Подробную информацию о том, как переместить данные из общего табличного пространства в табличное пространство file-per-table, см. в статье Перенос данных из общего табличного пространства в табличное пространство file-per-table в СУБД MySQL и MariaDB.

Настройка прав на восстановление данных Сервера администрирования

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

СУБД, основанная на PostgreSQL

В зависимости от способа создания базы данных Сервера предоставьте необходимые права роли, как описано в таблице ниже. Подробнее о настройке прав роли см. в статье Создание баз и учетных записей СУБД на основе PostgreSQL.

Права роли Postgres

Автоматическое создание базы данных		Создание базы данных вручную
Пользователю *Postgres* не требуются дополнительные права.	Права для новой роли: CREATEDB.	Для новой роли: • Права доступа к базе данных Сервера администрирования: ALL. • Права доступа ко всем таблицам в общедоступной схеме: ALL. • Права доступа ко всем последовательностям в общедоступной схеме: ALL.

Настройка прав на восстановление данных Сервера администрирования

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

На время восстановления данных из резервной копии предоставьте права суперпользователя Postgres для стандартных учетных записей klserver и kliam, которые Сервер администрирования и IAM используют для подключения к СУБД (в примере `klserver` и `kliam` соответственно):

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH SUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH SUPERUSER;"
```

После успешного восстановления данных восстановите исходные права у учетных записей Postgres.

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH NOSUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH NOSUPERUSER;"
```

Создание баз и учетных записей СУБД MySQL и MariaDB

Предварительные требования

Прежде чем создать базы данных и назначить права учетных записей СУБД, установите и настройте один из серверов в соответствии с требованиями оптимизации (если вы не выполнили это действие ранее):

- MariaDB x64 для работы с Kaspersky Security Center Linux
- MySQL x64 для работы с Kaspersky Security Center Linux

Не вносите вручную изменения в базу данных Сервера администрирования и базу данных IAM, включая изменение значений, удаление или добавление схем, таблиц, индексов. Любые изменения в базах данных, не выполненные самим Сервером администрирования, нарушают нормальную работу Сервера администрирования сразу или позже, например после обновления до более новой версии или при восстановлении из резервной копии. Изменение баз разрешено только в том случае, если вы получили точные инструкции от Службы технической поддержки "Лаборатории Касперского".
При деинсталляции или переносе Сервера на другое устройство вам нужно удалить базу данных вручную.

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:

   ```
   sudo mysql -u root -p
   ```

2. Создайте внутренние учетные записи СУБД с паролями. Приложение установки Сервера администрирования и службы Сервера администрирования используют эту внутреннюю учетную запись СУБД для доступа к СУБД.

   Создайте учетную запись Сервера администрирования с именем `kscdbadmin` и укажите пароль в значении `<password>`:

   ```
   CREATE USER 'kscdbadmin' IDENTIFIED BY '<password>';
   ```

3. Предоставьте следующие права созданной учетной записи СУБД:

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

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

   ```
   GRANT USAGE ON *.* TO 'kscdbadmin';
   ```

```
GRANT ALL ON kav.* TO 'kscdbadmin';
GRANT SELECT, SHOW VIEW ON mysql.* TO 'kscdbadmin';
GRANT SELECT, SHOW VIEW ON sys.* TO 'kscdbadmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin';
GRANT PROCESS ON *.* TO 'kscdbadmin';
GRANT SUPER ON *.* TO 'kscdbadmin';
```

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 'kscdbadmin'.
```

4. Для просмотра списка привилегий, предоставленных учетной записи СУБД, выполните следующую команду:

   ```
   SHOW grants for 'kscdbadmin';
   ```

5. Создайте учетную запись сервера IAM с именем `iamdbadmin` и укажите пароль в значении `<password>`:

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

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

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

6. 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:

   ```
   GRANT USAGE ON *.* TO 'iamdbadmin';
   GRANT ALL ON iam.* TO 'iamdbadmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'iamdbadmin';
   GRANT SELECT, SHOW VIEW ON sys.* TO 'iamdbadmin';
   GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin';
   GRANT PROCESS ON *.* TO 'iamdbadmin';
   GRANT SUPER ON *.* TO 'iamdbadmin';
   ```

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 'iamdbadmin'`.

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

   ```
   SHOW grants for 'iamdbadmin';
   ```

8. Создайте базу данных Сервера администрирования, выполнив следующую команду (в этом примере имя базы данных Сервера администрирования – *kav*):

   ```
   CREATE DATABASE kav
   ```

   Используйте то же имя базы данных, которое вы указали на шаге создания учетной записи СУБД.

9. Создайте базу данных IAM (в этом примере имя базы данных IAM – *iam*):

   ```
   CREATE DATABASE iam
   ```

Пример выполнения основных команд инструкции

```
administrator@ksclinux:~$ sudo mysql -u root -p

Enter password:

Welcome to the MySQL monitor. Commands end with ; or \g.

Your MySQL connection id is 8

Server version: 8.4.11-0ubuntu0.26.04.1 (Ubuntu)

Copyright (c) 2000, 2026, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its

affiliates. Other names may be trademarks of their respective

owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CREATE USER 'kscdbadmin' IDENTIFIED BY 'Your_P@$$w0rd';

Query OK, 0 rows affected (0.02 sec)

mysql> GRANT USAGE ON *.* TO 'kscdbadmin';

ON mysql.* TO 'kscdbadmin';

GRANT SELECT, SHOW VIEW ON sys.* TO 'kscdbadmin';

GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin';

GRANT PROCESS ON *.* TO 'kscdbadmin';

GRANT SUPER ON *.* TO 'kscdbadmQuery OK, 0 rows affected (0.00 sec)
```

```
mysql> GRANT ALL ON kav.* TO 'kscdbadmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT SELECT, SHOW VIEW ON mysql.* TO 'kscdbadmin';

Query OK, 0 rows affected (0.00 sec)

mysql> GRANT SELECT, SHOW VIEW ON sys.* TO 'kscdbadmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin';

in';

Query OK, 0 rows affected (0.00 sec)

mysql> GRANT PROCESS ON *.* TO 'kscdbadmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT SUPER ON *.* TO 'kscdbadmin';

Query OK, 0 rows affected, 1 warning (0.00 sec)

mysql> SHOW grants for 'kscdbadmin';

+-----------------------------------------------------------------------+

| Grants for kscdbadmin@% |

+-----------------------------------------------------------------------+

| GRANT PROCESS, SUPER ON *.* TO `kscdbadmin`@`%` |

| GRANT ALL PRIVILEGES ON `kav`.* TO `kscdbadmin`@`%` |

| GRANT SELECT, SHOW VIEW ON `mysql`.* TO `kscdbadmin`@`%` |

| GRANT SELECT, SHOW VIEW ON `sys`.* TO `kscdbadmin`@`%` |

| GRANT EXECUTE ON PROCEDURE `sys`.`table_exists` TO `kscdbadmin`@`%` |

+-----------------------------------------------------------------------+

5 rows in set (0.00 sec)

mysql> CREATE USER 'iamdbadmin' IDENTIFIED BY 'Your_P@$$w0rd';

Query OK, 0 rows affected (0.02 sec)

mysql> GRANT USAGE ON *.* TO 'iamdbadmin';
```

```
'iamdbadmin';

GRANT SELECT, SHOW VIEW ON sys.* TO 'iamdbadmin';

GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin';

GRANT PROCESS ON *.* TO 'iamdbadmin';

GRANT SUPER ON *.* TO 'iamdbaQuery OK, 0 rows affected (0.01 sec)

mysql> GRANT ALL ON iam.* TO 'iamdbadmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT SELECT, SHOW VIEW ON mysql.* TO 'iamdbadmin';

dmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT SELECT, SHOW VIEW ON sys.* TO 'iamdbadmin';

Query OK, 0 rows affected (0.02 sec)

mysql> GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT PROCESS ON *.* TO 'iamdbadmin';

Query OK, 0 rows affected (0.00 sec)

mysql> GRANT SUPER ON *.* TO 'iamdbadmin';

Query OK, 0 rows affected, 1 warning (0.00 sec)

mysql> SHOW grants for 'iamdbadmin';

+-----------------------------------------------------------------------+

| Grants for iamdbadmin@% |

+-----------------------------------------------------------------------+

| GRANT PROCESS, SUPER ON *.* TO `iamdbadmin`@`%` |

| GRANT ALL PRIVILEGES ON `iam`.* TO `iamdbadmin`@`%` |

| GRANT SELECT, SHOW VIEW ON `mysql`.* TO `iamdbadmin`@`%` |

| GRANT SELECT, SHOW VIEW ON `sys`.* TO `iamdbadmin`@`%` |

| GRANT EXECUTE ON PROCEDURE `sys`.`table_exists` TO `iamdbadmin`@`%` |
```

```
+--------------------------------------------------------------------+

5 rows in set (0.00 sec)

mysql> CREATE DATABASE kav;

Query OK, 1 row affected (0.01 sec)

mysql> CREATE DATABASE iam;

Query OK, 1 row affected (0.01 sec)

mysql> exit

Bye

administrator@ksclinux:~$
```

Создание баз и учетных записей СУБД на основе PostgreSQL

Перед назначением прав учетной записи СУБД убедитесь, что сервер СУБД на основе PostgreSQL настроен для работы с Kaspersky Security Center Linux.

Метод аутентификации Ident не поддерживается.

> Не вносите вручную изменения в базу данных Сервера администрирования и базу данных IAM, включая изменение значений, удаление или добавление схем, таблиц, индексов. Любые изменения в базах данных, не выполненные самим Сервером администрирования, нарушают нормальную работу Сервера администрирования сразу или позже, например после обновления до более новой версии или при восстановлении из резервной копии. Изменение баз разрешено только в том случае, если вы получили точные инструкции от Службы технической поддержки "Лаборатории Касперского".
> При деинсталляции или переносе Сервера на другое устройство, вам потребуется удалить базы данных Сервера администрирования и IAM вручную.

Чтобы создать базы данных и настроить учетные записи СУБД для установки Kaspersky Security Center Linux:

1. Запустите среду для работы с СУБД:

   `sudo -i -u postgres psql`

2. Выполните вход под пользователем *Postgres* в базу данных *Postgres*.

3. Создайте роль Postgres для работы с базой данных Сервера администрирования (в этом примере создается роль `kscdbadmin`):

   `CREATE USER "kscdbadmin" WITH PASSWORD '<password>';`

4. Создайте базу данных Сервера администрирования (в этом примере имя базы данных Сервера администрирования – `kav`):

   `CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";`

   Рекомендуется указать роль Postgres, созданную на шаге 3 этой инструкции, в качестве владельца базы данных Сервера администрирования (в этом примере роль – `kscdbadmin`, пароль – `<password>`).

   Указание другого пользователя в качестве владельца базы данных

Если вам нужно указать другую роль Postgres, подключитесь к базе данных Сервера администрирования под этой ролью владельца (или под ролью суперпользователя) и выполните следующие команды:

```
GRANT ALL PRIVILEGES ON DATABASE "kav" TO "kscdbadmin";
GRANT USAGE ON SCHEMA public TO "kscdbadmin";
GRANT CREATE ON SCHEMA public TO "kscdbadmin";
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "kscdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "kscdbadmin";
```

Убедитесь, что роль владельца базы данных Сервера администрирования имеет права CONNECT и TEMPORARY.

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

5. Создайте роль Postgres для работы с базой данных IAM (в этом примере создается роль Postgres – `iamdbadmin`):

```
CREATE USER "iamdbadmin" WITH PASSWORD '<password>';
```

6. Создайте базу данных IAM (в этом примере создается база данных IAM – `iam`):

```
CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";
```

Имя базы данных IAM должно отличаться от имени базы данных Сервера администрирования.

Рекомендуется указать роль Postgres, созданную на шаге 5 этой инструкции, в качестве владельца базы данных IAM (в этом примере роль – `iamdbadmin`, пароль – `<password>`).

Указание другого пользователя в качестве владельца базы данных IAM

Если вам нужно указать другую роль Postgres, подключитесь к базе данных IAM под этой ролью владельца (или под ролью суперпользователя) и выполните следующие команды:

```
GRANT ALL PRIVILEGES ON DATABASE "iam" TO "iamdbadmin";
GRANT USAGE ON SCHEMA public TO "iamdbadmin";
GRANT CREATE ON SCHEMA public TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "iamdbadmin";
```

Убедитесь, что роль владельца базы данных IAM имеет права CONNECT и TEMPORARY.

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

Пример выполнения основных команд инструкции

```
administrator@ksclinux:~$ sudo -i -u postgres psql
psql (18.4 (Ubuntu 18.4-0ubuntu.0.26.04.1))
Type "help" to help.
postgres=# CREATE USER kscdbadmin WITH PASSWORD 'password';
CREATE ROLE
postgres=# CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";
CREATE DATABASE
postgres=# CREATE USER iamdbadmin WITH PASSWORD 'password';
CREATE ROLE
postgres=# CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";
CREATE DATABASE
postgres=# exit
administrator@ksclinux:~$
```

Перенос данных из общего табличного пространства в табличное пространство file-per-table в СУБД MySQL или MariaDB

Для СУБД MySQL и MariaDB вы можете хранить данные следующими способами:

- В качестве общего табличного пространства, когда данные всех пользовательских баз данных хранятся в одном файле (обычно в файле `ibdata1`).
- В качестве табличного пространства file-per-table, когда для каждой таблицы создается отдельное пространство данных в виде отдельного файла.

Использование общего табличного пространства увеличивает риск фрагментации табличного пространства. Поскольку выполнить операцию `SHRINK` невозможно, файл в общем табличном пространстве может занимать около 90% дискового пространства. Это отрицательно сказывается на производительности дисковой подсистемы. Поэтому стоит выбрать табличное пространство file-per-table.

В этой статье описывается, как переместить данные из общего табличного пространства в табличное пространство file-per-table. Если СУБД MySQL или MariaDB также используются другими приложениями, вам необходимо переместить базы данных этих приложений в табличное пространство file-per-table.

> Рекомендуется выполнять перенос только в том случае, если вы используете СУБД MySQL или MariaDB для Сервера администрирования.
> Перемещение данных из общего табличного пространства в табличное пространство file-per-table может увеличить нагрузку на дисковую подсистему.

Предварительные требования

Перед тем как начать, убедитесь в следующем:

- Вы создали резервную копию данных Сервера администрирования, запустив либо задачу резервного копирования данных, либо утилиту klbackup.
- Вы создали резервную копию других приложений, базы данных которых управляются СУБД MySQL или MariaDB (если есть).
- На устройстве с установленной СУБД в разделе с базой данных есть свободное место на диске.

Требуемое дисковое пространство составляет 150% от текущего общего размера баз данных (текущего размера файла `ibdata1`).

Процесс

Чтобы переместить данные из общего табличного пространства в табличное пространство file-per-table:

1. Остановите службу Сервера администрирования Kaspersky Security Center и другие приложения, использующие экземпляр СУБД, для которого вы хотите выполнить эту процедуру.

2. В зависимости от версии СУБД войдите в свою СУБД как суперпользователь, а затем в любом приложении запустите скрипт `fix_tablespace.sql`.

   Вы можете просмотреть скрипты `fix_tablespace.sql`, перейдя по ссылкам:

   Просмотреть скрипт для MySQL 5.7 и MariaDB 10.1+

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;

DELIMITER //

CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()

BEGIN

    DECLARE __st_FETCH_STATUS INT;

    DECLARE `schemaName` VARCHAR(192);

    DECLARE `tableName` VARCHAR(192);

    DECLARE `curIX` CURSOR FOR

    SELECT `TABLE_SCHEMA` , `TABLE_NAME`

    FROM information_schema.TABLES

    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;


    OPEN `curIX`;

    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;

    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO

        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );

        PREPARE stmt1 FROM @`strSQL`;

        EXECUTE stmt1;

        DEALLOCATE PREPARE stmt1;


        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;

    END WHILE;

    CLOSE `curIX`;

END

//

DELIMITER ;

SET GLOBAL innodb_file_per_table = 1;
```

```
CALL upgd_alter_all_tables_for_all_databases_to_innodb();

DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

Просмотреть скрипт для MySQL 8.0+

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;

DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;

    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;

        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
innodb_file_per_table;' );
        PREPARE stmt2 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt2;

        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;

SET GLOBAL innodb_file_per_table = 1;

CALL upgd_alter_all_tables_for_all_databases_to_innodb();

DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

Не останавливайте выполнение скрипта.
Если ошибок СУБД не было, но вы прервали выполнение скрипта, либо запустите скрипт повторно, либо прекратите выполнение шагов этой процедуры, перезагрузите службу СУБД и восстановите данные Сервера администрирования из резервной копии.

3. В разделе `[mysqld]` файла my.cnf установите для параметра `innodb_file_per_table` значение `1`.

4. Перезагрузите службу MySQL или MariaDB.

5. Запустите службу Сервера администрирования Kaspersky Security Center.

Данные будут перемещены из общего табличного пространства в табличное пространство file-per-table:

Сертификаты для работы с Kaspersky Security Center Linux

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

О сертификатах Kaspersky Security Center

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

- сертификат Сервера администрирования;
- мобильный сертификат;
- сертификат Веб-сервера;
- сертификат Kaspersky Security Center Web Console;
- сертификат Identity and Access Manager (IAM).

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. При использовании пользовательского сертификата файл сертификата должен включать полную цепочку открытых ключей, включая все промежуточные сертификаты до корневого сертификата, подписанного аккредитованным центром сертификации (CA). 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 самоподписанный сертификат Сервер администрирования перевыпускает автоматически, а пользовательский сертификат вам необходимо будет заменить вручную по истечении срока его действия. Вы заменяете сертификаты на пользовательские с помощью утилиты klsetsrvcert в Kaspersky Security Center Web Console в свойствах Сервера администрирования, в зависимости от типа сертификата. При использовании утилиты klsetsrvcert необходимо указать тип сертификата, используя одно из следующих значений:

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

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

Сертификаты Сервера администрирования

Сертификат Сервера администрирования необходим для следующих целей:

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

Сертификат Сервера администрирования автоматически создается при установке компонента Сервер администрирования и хранится в каталоге /var/opt/kaspersky/klnagent_srv/1093/cert/. Сертификат Сервера администрирования вы указываете при создании файла ответов для установки Kaspersky Security Center Web Console. Этот сертификат называется общим ("C"). После установки Kaspersky Security Center Web Console заданный вами сертификат копируется в каталог /var/opt/kaspersky/ksc-web-console/certificates/external/

Сертификат Сервера администрирования действителен 397 дней. Kaspersky Security Center автоматически создает 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 переподключения Агентов администрирования.

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

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 90 дней до истечения срока действия мобильного сертификата. Когда истекает срок действия мобильного сертификата, мобильный резервный сертификат используется для поддержания связи с Агентами администрирования, установленными на управляемых мобильных устройствах. С этой целью мобильный резервный сертификат автоматически становится новым мобильным сертификатом за 24 часа до истечения срока действия старого мобильного сертификата.

Если сценарий подключения требует использования сертификата клиента на мобильных устройствах (подключение с двусторонней SSL-аутентификацией), 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 доверенным центром сертификации, при условии, что интеграция с инфраструктурой открытых ключей (PKI) вашей организации позволяет выпускать сертификаты клиентов с помощью центра сертификации домена.

Также для аутентификации Сервера администрирования на мобильных устройствах, работающих под управлением операционной системы iOS, требуется сертификат Сервера iOS MDM. 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 загрузки 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 Web Console

Сервер Kaspersky Security Center Web Console (далее также Web Console) имеет собственный сертификат. При открытии сайтов 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 отображается 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.

По умолчанию срок действия самоподписанного сертификата составляет 30 дней. Вы можете изменить это значение файле в конфигурации веб-консоли /var/opt/kaspersky/ksc-web-console/server/config.json Чтобы применить заданное значение, вам потребуется перезапустить процесс Web Console.

Web Console автоматически до истечениия срока действия самоподписанного сертификат перевыпускает этот сертификат и переключается на него.

Вы можете заменить самоподписанный сертификат Web Console на пользовательский.

Сертификат Identity and Access Manager (IAM)

Сертификат Identity and Access Manager (IAM-сертификат) необходим для следующих целей:

- Проверка подлинности Сервера администрирования, когда браузер пользователя подключается к нему по протоколу OAuth.

- Аутентификация Сервера администрирования при подключении к нему Kaspersky Security Center Web Console.

IAM-сертификат создается автоматически при первом запуске Сервера администрирования. Сертификат хранится на устройстве с Сервером администрирования в каталоге: /var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem (для отказоустойчивого кластера Kaspersky Security Center: <общая папка данных>/iam/main_certificate.pem). Вам нужно указать путь к IAM-сертификату с помощью параметра `iamCertPath` при создании файла ответов для установки Kaspersky Security Center Web Console.

IAM-сертификат действителен в течение 365 дней. Kaspersky Security Center автоматически создает резервный IAM-сертификат за 48 часов до истечения срока действия текущего сертификата. Резервный сертификат впоследствии используется для замены IAM-сертификата.

Максимальный срок действия любого IAM-сертификата не должен превышать 397 дней.

При необходимости вы можете назначить пользовательский IAM-сертификат. Например, это может понадобиться для лучшей интеграции с существующей PKI вашей организации или для требуемой настройки полей сертификата.

При входе в Kaspersky Security Center Web Console браузер перенаправляется на страницу входа в Сервер администрирования (https://< `адрес Сервера администрирования`>: 4444) для аутентификации. Трафик между браузером и Сервером администрирования шифруется с помощью TLS-протокола и IAM-сертификата.

Браузер может сообщить вам, что подключение к Серверу администрирования не является безопасным и IAM-сертификат недействителен. Это предупреждение появляется, потому что IAM-сертификат является самоподписанным и автоматически генерируется Kaspersky Security Center. Чтобы удалить это предупреждение, можно выполнить одно из следующих действий:

- Заменить IAM-сертификат на пользовательский сертификат (рекомендуемый параметр). Создать сертификат, доверенный в вашей инфраструктуре и соответствующий требованиям к пользовательским сертификатам.

- Добавить IAM-сертификат 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 Linux

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

Требования для сертификатов Kaspersky Security Center Linux

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. Сертификат должен включать допустимое альтернативное имя субъекта (Subject Alternative Name, SAN), которое содержит адрес Сервера администрирования для обратной связи: • Для IPv4: 127.0.0.1 • Для IPv6: 0:0:0:0:0:0:0:1	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 полную цепочку открытых ключей. Присутствует альтернативное имя субъекта (SAN) сертификата; то есть значение поля `subjectAltName` является допустимым. Сертификат соответствует действующим требованиям браузеров, предъявляемым к сертификатам серверов, а также к текущим базовым требованиям CA/Browser Forum.	—

Тип сертификата	Требования	Комментарии
Сертификат Kaspersky Security Center Web Console	Расширенное использование ключа (Extended Key Usage, EKU): аутентификация сервера. Контейнер PEM, из которого указывается сертификат, включает полную цепочку открытых ключей. Присутствует альтернативное имя субъекта (SAN) сертификата; то есть значение поля `subjectAltName` является допустимым. Значение должно совпадать с адресом IAM, указанным при установке Сервера администрирования. Для получения указанного адреса IAM выполните следующую команду на устройстве с установленным Сервером администрирования: `grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` Сертификат соответствует действующим требованиям браузеров к сертификатам серверов, а также к текущим базовым требованиям CA/Browser Forum.	Зашифрованные сертификаты не поддерживаются Kaspersky Security Center Web Console.
Сертификат Identity and Access Manager (IAM-сертификат)	Расширенное использование ключа (EKU): аутентификация сервера. Контейнер PEM, из которого указывается сертификат, включает полную цепочку открытых ключей. Сертификат соответствует действующим требованиям браузеров к сертификатам серверов, а также к текущим базовым требованиям CA/Browser Forum.	Зашифрованные сертификаты не поддерживаются Kaspersky Security Center Web Console.

Перевыпуск внутренних сертификатов для Kaspersky Security Center Web Console

Kaspersky Security Center Web Console использует следующие сертификаты:

- публичный (TLS-сертификат Web Console), который Web Console предъявляет браузеру при HTTPS-соединении;
- внутренний, с помощью которого Web Console организовывает TLS-соединение.

Публичный сертификат

Большинство браузеров ограничивает срок действия сертификата. Чтобы попасть в это ограничение, срок действия публичного сертификата в Kaspersky Security Center Web Console равен 30 дням. Вы можете заменить существующий сертификат, полученный от доверенного центра сертификации (CA), при выпуске вручную нового самоподписанного сертификата.

Если вы выбрали создать сертификат, при открытии Kaspersky Security Center Web Console браузер может информировать вас о том, что подключение к Kaspersky Security Center Web Console не является приватным и что сертификат Kaspersky Security Center Web Console недействителен. Это предупреждение появляется потому, что сертификат Kaspersky Security Center Web Console является самоподписанным и автоматически генерируется Kaspersky Security Center. Чтобы удалить или предотвратить это предупреждение, можно выполнить одно из следующих действий:

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

Внутренний сертификат

Внутренний сертификат Web Console служит только для внутренней взаимной аутентификации компонентов Web Console и не отображается пользователю.

По умолчанию срок действия внутреннего сертификата Kaspersky Security Center Web Console составляет 3 года (1095 дней).

За 14 дней до истечения указанного срока в Web Console отображается уведомление о необходимости перевыпустить внутренний сертификат.

Чтобы перевыпустить внутренний сертификат Kaspersky Security Center Web Console:

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

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

Сертификат Kaspersky Security Center Web Console перевыпущен.

Замена сертификата для Kaspersky Security Center Web Console

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

Чтобы назначить пользовательский сертификат Kaspersky Security Center Web Console:

1. Сохраните файл с сертификатом и файл с закрытым ключом в каталоге:

   /var/opt/kaspersky/ksc-web-console/certificates/external/

   Поддерживаемый формат файлов: PEM.
   Пользователь с правами root имеет право на чтение и запись в каталоге. Пользователь, от имени которого запускается сервис интерактивной веб-консоли, имеет право только на чтение.

2. Присвойте файлам следующие имена:

   - web-console.crt – файл с сертификатом;
   - web-console.key – файл с закрытым ключом без пароля.

Пользовательский основной сертификат назначен и Web Console использует его.

Если вы захотите заменить пользовательский сертификат:

- на другой пользовательский, выполните эту же инструкцию.
- на самоподписанный, удалите один либо оба файла пользовательского сертификата.

По истечении срока действия пользовательского сертификата Web Console отображает соответствующее уведомление и продолжает использовать истекший сертификат.

Если заданный вами пользовательский основной сертификат недействителен, Web Console отображает соответствующее уведомление, выпускает самоподписанный основной и переключается на него.

Уведомление начинает отображаться за 14 дней до истечения сертификата.

Преобразование сертификата из формата PFX в формат PEM

Чтобы использовать сертификат формата PFX в Kaspersky Security Center Web Console, вам необходимо предварительно преобразовать его в формат PEM с помощью любой кроссплатформенной утилиты на основе OpenSSL.

Чтобы преобразовать сертификат из формата PFX в формат PEM в операционной системе Linux:

1. В кроссплатформенной утилите на основе OpenSSL выполните следующие команды:

   ```
   openssl pkcs12 -in <file_name.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <file_name.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Убедитесь, что файл сертификата и закрытый ключ сгенерированы в той же папке, где хранится файл PFX.

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

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

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

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

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

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

Должны быть соблюдены следующие условия:

- Сертификат должен быть создан в формате PKCS#12 (например, с помощью PKI организации).
- Для нового сертификата должны быть соблюдены требования, перечисленные в таблице ниже.

  В таблице ниже обратите внимание на требование "CA: true". Оно означает, что новый сертификат должен быть выдан доверенным центром сертификации (CA). Новый сертификат с требованием "CA: true" должен включать в себя всю цепочку доверия и закрытый ключ, который должен храниться в файле с расширением pfx или p12.

Требования к сертификатам Сервера администрирования

Тип сертификата	Требования
Общий сертификат, общий резервный сертификат ("C", "CR")	Минимальная длина ключа: 2048. Основные ограничения: • Ограничение длины пути: Отсутствует. Значение ограничения длины пути может быть целым числом отличным от "None", но не 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. Сертификат должен включать допустимое альтернативное имя субъекта (Subject Alternative Name, SAN), которое содержит адрес Сервера администрирования для обратной связи: • Для IPv4: 127.0.0.1 • Для IPv6: 0:0:0:0:0:0:0:1

Тип сертификата	Требования
Мобильный сертификат, мобильный резервный сертификат ("M", "MR")	Минимальная длина ключа: 2048. Основные ограничения: • CA: true. • Ограничение длины пути: Отсутствует. Значение ограничения длины пути может быть целым числом, отличным от "None", если Общий сертификат имеет значение ограничения длины пути не менее 1. Использование ключа: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (EKU): аутентификация сервера. EKU необязательно, но если оно содержится в вашем сертификате, данные аутентификации сервера должны быть указаны в EKU.
Сертификат, выпущенный доверенным центром сертификации (CA), для автоматически генерируемых пользовательских сертификатов (MCA)	Минимальная длина ключа: 2048. Основные ограничения: • CA: true. • Ограничение длины пути: Отсутствует. Значение ограничения длины пути может быть целым числом, отличным от "None", если Общий сертификат имеет значение ограничения длины пути не менее 1. Использование ключа: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (англ. Extended Key Usage, EKU): аутентификация клиента. EKU необязателен, но если он содержится в вашем сертификате, данные аутентификации клиента должны быть указаны в EKU.

Сертификаты, выпущенные 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.

3. **Указание нового сертификата в каталоге с сертификатами Kaspersky Security Center Web Console**

   Сохраните файл с сертификатом Сервера администрирования в каталоге:/var/opt/kaspersky/ksc-web-console/certificates/external/

Присвойте файлу имя <address>-admin-server.crt, где <address> – адрес Сервреа администрирования который вы задали в параметре `iamHost` файла ответов инсталлятора Web Console.

Поддерживаемый формат файла: PEM.
Пользователь с правами root имеет право на чтение и запись в каталоге. Пользователь, от имени которого запускается сервис интерактивной веб-консоли, имеет право только на чтение.

Результаты

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

Замена сертификата Сервера администрирования с помощью утилиты klsetsrvcert

Ознакомьтесь со статьей Сценарий: задание пользовательского сертификата Сервера администрирования, прежде чем продолжить, иначе вы можете потерять контроль над устройствами.

Чтобы заменить сертификат Сервера администрирования:

В командной строке выполните следующую команду:

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert [-t <certificate type> {-i <path to new certificate> [-p <password>] [-o
<validation parameters>] | -g <dns name>}][-f <replacement time>][-r <root certificates>][-l <log file path>]
```

Описание параметров утилиты klsetsrvcert представлено в таблице ниже.

Значения параметров утилиты klsetsrvcert

Параметр	Значение
`-t <certificate type>`	Тип сертификата, который следует заменить. Возможные значения параметра `<certificate type>`: • `C` – заменить общий сертификат для портов 13000 и 13291. • `CR` – заменить общий резервный сертификат для портов 13000 и 13291.
`-f <replacement 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 <path to the new certificate>`	Контейнер с сертификатом и закрытый ключ в формате PKCS#12 (файл с расширением p12 или pfx).
`-p <password>`	Пароль, при помощи которого защищен p12-контейнер. Сертификат и закрытый ключ хранятся в контейнере, поэтому для расшифровки файла с контейнером требуется пароль.

Параметр	Значение
`-o <validation parameters>`	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:<key length>`, где параметр `<key length>` – это необходимая длина ключа. Иначе используется текущая длина ключа сертификата.
`-g <DNS name>`	Новый сертификат будет создан для указанного DNS-имени (Common Name и Subject Alternative Name).
`-r <root certificates>`	Список доверенных корневых сертификатов, подписанных доверенным центром сертификации, в формате PEM.
`-l <path to the log file>`	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 <path to the new certificate> -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 <путь к новому сертификату> -p <пароль> -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.

Вопросы и ответы

Какие дополнительные действия необходимо выполнить после замены общего сертификата Сервера администрирования?

1. Убедитесь, что **соблюдены требования к пользовательским сертификатам**.

   Если вы используете пользовательский сертификат вместо самоподписанного, перед обновлением Kaspersky Security Center Linux до более поздней версии вам нужно убедиться, что сертификат содержит альтернативное имя субъекта (Subject Alternative Name, SAN). Если нет, важно заменить сертификат перед обновлением Kaspersky Security Center Linux. Иначе вы не сможете войти в Web Console после обновления.

Чтобы убедиться, что сертификат включает SAN:

1. На устройстве, на котором установлен Сервер администрирования, выполните команду:

   - Для устройств с операционной системой Linux:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   - Для устройств с операционной системой Windows:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Убедитесь, что альтернативное имя субъекта (SAN) присутствует в выходных данных команды и содержит адрес устройства Сервера администрирования.

3. Если альтернативное имя субъекта отсутствует, используйте утилиту klsetsrvcert для замены пользовательского сертификата на сертификат, который соответствует требованиям.

2. Убедитесь, что конфигурационный файл сервера IAM содержит текущий адрес Сервера администрирования. Если нет, добавьте адрес в конфигурационный файл.

3. Переустановите Web Console, чтобы избежать следующей ошибки:

   Сервер администрирования использует недоверенный сертификат. Перенастройте приложение, указав действительный сертификат, или обратитесь к главному администратору.

Подключение Агентов администрирования к Серверу администрирования с помощью утилиты klmover

Вы можете использовать утилиту klmover для восстановления подключения неконтролируемых устройств к Серверу администрирования, например, если после сбоя Сервера администрирования невозможно восстановить подключение из резервной копии.

Чтобы восстановить подключение, запустите утилиту klmover из командной строки:

- Для Linux:

  - Для 32-разрядной системы: `/opt/kaspersky/klnagent/bin/klmover [-address <адрес сервера>] [-pn <номер порта>] [-ps <номер TLS-порта>] [-nossl] [-cert <путь к файлу сертификата>]`

  - Для 64-разрядной системы: `/opt/kaspersky/klnagent64/bin/klmover [-address <адрес сервера>] [-pn <номер порта>] [-ps <номер TLS-порта>] [-nossl] [-cert <путь к файлу сертификата>]`

- Для Windows:

  - Для 32-разрядной системы: `<путь>\klmover.exe [-address <адрес сервера>] [-pn <номер порта>] [-ps <номер TLS-порта>] [-nossl] [-cert <путь к файлу сертификата>]`

  - Для 64-разрядной системы: `<путь>\klmover.exe [-address <адрес сервера>] [-pn <номер порта>] [-ps <номер TLS-порта>] [-nossl] [-cert <путь к файлу сертификата>]`

- Для macOS:

  ```
  /Library/Application Support/Kaspersky Lab/klnagent/Binaries/klmover [-address <адрес сервера>] [-pn <номер порта>] [-ps <номер TLS-порта>] [-nossl] [-cert <путь к файлу сертификата>]
  ```

  где <путь> – это путь установки по умолчанию Агента администрирования или путь установки, указанный вами в параметрах инсталляционного пакета Агента администрирования.

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

Если вы потеряли или забыли пароль от Агента администрирования, установленного на устройстве и защищенного паролем, которое больше не находится под управлением Kaspersky Security Center Linux, вы не сможете удалить этот Агент администрирования с помощью утилиты klmover или с помощью командной строки. В этом случае необходимо переустановить операционную систему на устройстве с установленным Агентом администрирования, защищенным паролем.

Утилита klmover требует прав локального администратора.

При включении параметра **Использовать пароль деинсталляции** на устройствах с операционной системой Windows также включается защита паролем средствами Cleaner (cleaner.exe).

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 TLS-порта>`	Номер TLS-порта, по которому осуществляется зашифрованное подключение к Серверу администрирования с использованием протокола TLS. По умолчанию установлен порт 13000.
`-nossl`	Использовать незашифрованное подключение к Серверу администрирования. Если ключ не используется, подключение Агента администрирования к Серверу осуществляется по защищенному TLS-протоколу.
`-cert <путь к файлу сертификата>`	Использовать указанный файл сертификата для аутентификации доступа к Серверу администрирования.
`-nauninstpwd <пароль>`	Используйте этот параметр, чтобы указать пароль для деинсталляции Агента администрирования. Необязательный параметр.

Перевыпуск сертификата Веб-сервера

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

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

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

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

1. Создайте пользовательский сертификат и подготовьте его для использования в Kaspersky Security Center Linux. Проверьте, соответствует ли ваш пользовательский сертификат требованиям Kaspersky Security Center Linux. При необходимости измените сертификат.

2. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

3. На вкладке **Общие** выберите раздел **Веб-сервер**.

4. В подразделе **По протоколу HTTP** выберите вариант **Загрузить сертификат из файла** и нажмите на кнопку **Изменить сертификат**.

5. В открывшемся окне в поле **Формат сертификата** выберите тип вашего сертификата:

   - Если вы выбрали **Контейнер PKCS#12**, нажмите на кнопку **Обзор** рядом с полем **Сертификат** и укажите файл сертификата на жестком диске. Если файл сертификата защищен паролем, введите пароль в поле **Пароль**.

   - Если вы выбрали **X.509-сертификат**, нажмите на кнопку **Обзор** рядом с полем **Закрытый ключ** и укажите закрытый ключ на жестком диске. Если закрытый ключ защищен паролем, введите пароль в поле **Пароль**.

6. Нажмите на кнопку **Сохранить** и далее на кнопку **OK**.

   Окно закрыто.

7. При необходимости в поле **HTTPS-порт Веб-сервера** измените номер HTTPS-порта для Веб-сервера и нажмите на кнопку **Сохранить**.

Сертификат Веб-сервера перевыпущен.

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

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Сертификаты**.

3. Если вы планируете и дальше использовать сертификат, выданный Kaspersky Security Center:

   a. Выберите вариант **Сертификат выпущен средствами Сервера администрирования** и нажмите на кнопку **Обзор**.

   b. В открывшемся окне блоках параметров **Адрес подключения** и **Срок активации** выберите соответствующие параметры и нажмите на кнопку **OK**.

Если вы планируете использовать собственный сертификат, выполните следующее:

a. Проверьте, соответствует ли ваш пользовательский сертификат требованиям Kaspersky Security Center Linux. При необходимости измените сертификат.

b. Выберите вариант **Другой сертификат**, нажмите на кнопку **Управление сертификатом** и в открывшемся окне нажмите на кнопку **Обзор**.

c. В открывшемся окне в поле **Формат сертификата** выберите тип вашего сертификата:

   - Если вы выбрали **Контейнер PKCS#12**, нажмите на кнопку **Обзор** рядом с полем **Сертификат** и укажите файл сертификата на жестком диске. Если файл сертификата защищен паролем, введите пароль в поле **Пароль**.

   - Если вы выбрали **X.509-сертификат**, нажмите на кнопку **Обзор** рядом с полем **Закрытый ключ** и укажите закрытый ключ на жестком диске. Если закрытый ключ защищен паролем, введите пароль в поле **Пароль**.

d. Нажмите на кнопку **Сохранить** и далее на кнопку **OK**.

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

Замена IAM-сертификата по умолчанию на пользовательский сертификат

Чтобы назначить пользовательский IAM-сертификат:

1. Создайте пользовательский сертификат и подготовьте его для использования в Kaspersky Security Center Linux. Проверьте, соответствует ли ваш пользовательский сертификат требованиям Kaspersky Security Center Linux.

2. Убедитесь, что группа kladmins имеет доступ к файлам IAM-сертификатов.

3. Откройте конфигурационный файл IAM: `/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`.

   В этом файле добавьте пути к файлам IAM-сертификатов в секции `server_iam`:

   - `certificates.main.cert`: Путь к файлу действительного сертификата.
   - `certificates.main.key`: Путь к закрытому ключу действительного сертификата. Закрытый ключ не должен быть защищен паролем.

4. Перезапустите сервис kliam, выполнив следующую команду:

   ```
   sudo service kliam_srv restart
   ```

5. Сохраните файл с сертификатом IAM в каталоге:

   /var/opt/kaspersky/ksc-web-console/certificates/external/

   > Поддерживаемый формат файла: PEM.
   > Учетная запись, от имени которой запущена служба Kaspersky Security Center Web Console, должна иметь право на чтение файлов, сохраненных в каталоге.

6. Присвойте файлу имя: <address>-iam-server.crt

   где <address> – адрес IAM, который вы задали в параметре `iamHost` файла ответов инсталлятора Web Console.

Пользовательский IAM-сертификат назначен, и Web Console использует его.

При необходимости заменить пользовательский IAM-сертификат, выполните эту же инструкцию.

Если заданный вами IAM-сертификат недействителен и новый действительный сертификат не получен, в Web Console отображается ошибка.

По умолчанию за 14 дней до истечения действующего сертификата отображается предупреждающее уведомление. За 2 дня до истечения действующего сертификата отображается критическое уведомление.

Если после того, как вы вручную указали для Web Console IAM-сертификат (самоподписанный либо пользовательский), IAM переключился на резервный сертификат, Web Console автоматически получит резервный сертификат IAM и продолжит подключаться к Серверу администрирования. При этом указанный вами пользовательский сертификат останется в каталоге /var/opt/kaspersky/ksc-web-console/certificates/external/, но не будет использоваться.

Чтобы изменить резервный IAM-сертификат:

1. Откройте конфигурационный файл IAM: `/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`.

   В этом файле укажите пути к файлам IAM-сертификатов:

   - `server_iam.certificates.reserve.cert`: Путь к файлу действительного сертификата.
   - `server_iam.certificates.reserve.key`: Путь к закрытому ключу действительного сертификата. Закрытый ключ не должен быть защищен паролем.

2. Перезапустите сервис kliam, выполнив следующую команду:

   ```
   sudo systemctl restart kliam_srv.service
   ```

   После истечения срока действия текущего файла сертификата вместо него используется резервный IAM-сертификат.

Добавление адреса Сервера администрирования в конфигурацию сервера IAM

После изменения общего сертификата Сервера администрирования ("C") во время обновления, перемещения или переноса данных, вам нужно указать адрес Сервера администрирования в конфигурационном файле сервера IAM, чтобы обеспечить правильную проверку сертификата между сервером IAM и Сервером администрирования.

Чтобы добавить адрес Сервера администрирования в конфигурацию сервера IAM:

1. Получите значение альтернативного имени субъекта (SAN) из общего сертификата Сервера администрирования ("C"), выполнив следующую команду:

   ```
   sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
   ```

2. В зависимости от выходных данных команды выполните одно из следующих действий:

   - Если в выходных данных указано, что значение отсутствует или содержит только сетевой IP-адрес, проверьте **требования к пользовательскому сертификату**.

     Если вы используете пользовательский сертификат вместо самоподписанного, перед обновлением Kaspersky Security Center Linux до более поздней версии вам нужно убедиться, что сертификат содержит альтернативное имя субъекта (Subject Alternative Name, SAN). Если нет, важно заменить сертификат перед обновлением Kaspersky Security Center Linux. Иначе вы не сможете войти в Web Console после обновления.

     Чтобы убедиться, что сертификат включает SAN:

     1. На устройстве, на котором установлен Сервер администрирования, выполните команду:

        - Для устройств с операционной системой Linux:

          ```
          sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
          ```

        - Для устройств с операционной системой Windows:

          ```
          certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
          ```

2. Убедитесь, что альтернативное имя субъекта (SAN) присутствует в выходных данных команды и содержит адрес устройства Сервера администрирования.

3. Если альтернативное имя субъекта отсутствует, используйте утилиту klsetsrvcert для замены пользовательского сертификата на сертификат, который соответствует требованиям.

Если сертификат не соответствует требованиям, замените общий сертификат Сервера администрирования на предыдущем Сервере администрирования с помощью утилиты klsetsrvcert. После этого повторите процедуру обновления с предыдущей версии, перемещения или переноса данных.

- Если значение совпадает со значением, указанным при установке Kaspersky Security Center Linux (на шаге **Ввод DNS-имени сервера IAM** мастера установки или для тихой установки в параметре `KLSRV_UNATT_IAM_ADDRESS`), никаких дополнительных действий не требуется. Сервер IAM и Сервер администрирования будут правильно взаимодействовать.

- Если значение содержит DNS-имена или адреса обратной связи (127.0.0.1 и/или 0:0:0:0:0:0:0:1), используйте один из них в конфигурационном файле. Рекомендуется использовать 127.0.0.1.

3. В блоке `server_iam` конфигурационного файла сервера IAM убедитесь, что значение `ksc_address: "<SAN_address>"` соответствует одному из SAN-адресов в общем сертификате Сервера администрирования.

   Вы можете использовать текстовый редактор для изменения конфигурационного файла сервера IAM, например, vi. Следующая команда открывает файл в текстовом редакторе vi:

   ```
   vi /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
   ```

   Пример блока server_iam в конфигурационном файле сервера IAM:

   ```
   server_iam:
       iam_address: "ksc.example.com"
       server_display_name: "ksc.example.com"
       ksc_address: "oldksc.example.internal"
       ksc_ca: "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
   ```

   Убедитесь, что вы используете тот же интервал, что и в примере.

4. Убедитесь, что сетевое имя в параметре `ksc_address` разрешается в адрес обратной связи (127.0.0.1 и/или 0:0:0:0:0:0:0:1) Сервера администрирования. Для этого вы можете использовать утилиту Ping на Сервере администрирования.

   Если разрешенный адрес отличается или адрес не удается разрешить, добавьте запись в файл hosts на Сервере администрирования.

5. Чтобы применить изменения конфигурации, перезапустите службу сервера IAM, выполнив следующую команду:

   ```
   sudo systemctl restart kliam_srv.service
   ```

Адрес Сервера администрирования добавлен в конфигурационный файл сервера IAM из общего сертификата Сервера администрирования.

Устранение неисправностей

Наличие в сети нескольких Серверов администрирования с одинаковыми сетевыми именами и проблемы с конфигурацией сервера IAM могут приводить к ошибкам при входе в Web Console. В таблице ниже описаны возможные ошибки и способы их устранения.

Сбой	Описание	Решение
Ваш запрос в настоящее время не может быть обработан. Пожалуйста, подождите и попробуйте позже.	Помимо процесса инициализации данных после обновления или восстановления Kaspersky Security Center Linux, эта ошибка может возникать в случае сбоя подключения к Серверу администрирования по указанному сетевому адресу.	Убедитесь, что указанный адрес разрешается в IP-адрес текущего Сервера администрирования.
Сервер администрирования использует недоверенный сертификат. Перенастройте приложение, указав действительный сертификат, или обратитесь к главному администратору.	Ошибка может возникнуть, если значение адреса в конфигурационном файле сервера IAM не соответствует значению в атрибуте Альтернативное имя субъекта (SAN) общего сертификата Сервера администрирования.	Следуйте инструкциям выше.
Имя пользователя или пароль неверны.	Помимо неверных учетных данных, эта ошибка может возникнуть, если в сети существует другой Сервер администрирования с таким же именем.	Убедитесь, что указанный адрес разрешается в IP-адрес текущего Сервера 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.

Вход в приложение Kaspersky Security Center Web Console и выход из него

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

Вы можете войти в Kaspersky Security Center Web Console следующими способами:

- С помощью доменной аутентификации (единый вход).

  Этот способ используется для безопасной аутентификации в приложении Kaspersky Security Center Web Console, подключенном к Серверу администрирования версии 16 и выше. Если вы хотите использовать доменную аутентификацию, вам нужно указать дополнительные параметры для взаимодействия с Identity and Access Manager (IAM) при установке Kaspersky Security Center Web Console.

- Указав имя пользователя и пароль доменного пользователя.

  Прежде чем войти в систему с использованием доменной учетной записи пользователя, опросите контроллеры домена, чтобы получить список пользователей домена. Затем нужно указать имя доменного пользователя и пароль для входа на Сервер администрирования. Этот способ поддерживается для аутентификации только через Microsoft Active Directory.

- Указав имя пользователя и пароль внутреннего пользователя.

Учетной записи пользователя, под которой вы хотите войти в Kaspersky Security Center Web Console, должна быть назначена роль. Прежде чем войти в приложение убедитесь, что доменной учетной записи или внутренней учетной записи пользователя назначена роль. Иначе возникнет ошибка.

Вход с использованием доменной аутентификации (единый вход)

Чтобы войти в Kaspersky Security Center Web Console, используя доменную аутентификацию:

1. В вашем браузере перейдите по ссылке https://`<Kaspersky Security Center Web Console address>`:`<Port number>`.

   Откроется страница выбора Сервера администрирования.

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

   Если вы добавили только один Сервер администрирования, список Серверов администрирования не отображается.

   Браузер перенаправляется на https://`< Administration Server address>`: 4444.

3. Настройте доменную аутентификацию Kerberos.

4. Выполните одно из следующих действий:

   - Нажмите на кнопку **Использовать доменную аутентификацию**.

   - Если на Сервере создан один или несколько виртуальных Серверов администрирования и вы хотите войти на виртуальный Сервер с использованием доменной аутентификации:

     a. Нажмите на кнопку **Показать параметры виртуального Сервера**.

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

     c. Нажмите на кнопку **Использовать доменную аутентификацию**.

5. Введите одноразовый код безопасности, сгенерированный в приложении для аутентификации на мобильном устройстве.

   При первом входе настройте двухэтапную аутентификацию для своей учетной записи. Если вам недоступна настройка двухфакторной аутентификации, обратитесь к пользователю, у которого есть право Изменение списков управления доступом объектов в функциональной области **Общие функции**: **Права пользователей** и который настроил двухфакторную аутентификацию, чтобы добавить вашу учетную запись в список пользователей с правом настраивать двухфакторную аутентификацию.

После входа отобразится домашняя страница Kaspersky Security Center Web Console, язык интерфейса и тема будут такими, которые вы использовали в последний раз. Вы можете перемещаться по Kaspersky Security Center Web Console и использовать ее для работы с Kaspersky Security Center Linux.

Вход с использованием имени и пароля доменного или внутреннего пользователя

Чтобы войти в Kaspersky Security Center Web Console, указав имя учетной записи и пароль:

1. В вашем браузере перейдите по ссылке https://`<Kaspersky Security Center Web Console address>`:`<Port number>`.

   Откроется страница выбора Сервера администрирования.

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

   Если вы добавили только один Сервер администрирования, список Серверов администрирования не отображается.

   Браузер перенаправляется на https://< `Administration Server address`>: 4444.

3. Выполните одно из следующих действий:

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

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

     - `User name@dns.domain`
     - `NTDOMAIN\User name`

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

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

- Если на Сервере создан один или несколько виртуальных Серверов администрирования и вы хотите войти на виртуальный Сервер:

  a. Нажмите на кнопку **Показать параметры виртуального Сервера**.

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

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

4. Нажмите на кнопку **Войти**.

5. Введите одноразовый код безопасности, сгенерированный в приложении для аутентификации на мобильном устройстве.

   При первом входе настройте двухэтапную аутентификацию для своей учетной записи. Если вам недоступна настройка двухфакторной аутентификации, обратитесь к пользователю, у которого есть право Изменение списков управления доступом объектов в функциональной области **Общие функции**: **Права пользователей** и который настроил двухфакторную аутентификацию, чтобы добавить вашу учетную запись в список пользователей с правом настраивать двухфакторную аутентификацию.

6. Если для вашей учетной записи включено принудительное изменение пароля или срок действия пароля истек, отобразится окно изменения пароля. Установите новый пароль для входа в Kaspersky Security Center Web Console.

После входа отобразится домашняя страница Kaspersky Security Center Web Console, язык интерфейса и тема будут такими, которые вы использовали в последний раз. Вы можете перемещаться по Kaspersky Security Center Web Console и использовать ее для работы с Kaspersky Security Center Linux.

Выход

Чтобы выйти из Kaspersky Security Center Web Console,

В верхней панели откройте меню своей учетной записи, нажав на ее имя и выберите **Выход**.

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

Интерфейс Kaspersky Security Center Web Console

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

Окно приложения Kaspersky Security Center Web Console содержит следующие элементы:

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

Главное меню

Главное меню содержит следующие разделы:

- **Сервер администрирования**. Отображает имя Сервера администрирования, к которому вы сейчас подключены. Вы можете открыть свойства Сервера администрирования, нажав на имя Сервера администрирования.
- **Навигация консоли**. Отображает карту главного меню. Большинство отображаемых разделов можно добавить в закладки или установить в качестве домашней страницы. Раздел **Навигация консоли** установлен как домашняя страница по умолчанию. Вы можете изменить эти параметры.
- **Мониторинг**. Предоставляет сведения об инфраструктуре вашей сети, статусе защиты, а также статистику.
- **Управление активами**. Содержит инструменты для управления устройствами и оборудованием, а также политиками приложений "Лаборатории Касперского".
- **Задачи**. Содержит инструменты для создания и запуска задач.
- **Пользователи и роли**. Позволяет управлять пользователями и ролями, настраивать права пользователей, назначать пользователям роли и связывать профили политик с ролями.
- **Хранилища**. Предоставляет вам доступ к хранилищам приложений.
- **Управление программным обеспечением**. Позволяет управлять приложениями "Лаборатории Касперского" и приложениями сторонних производителей, а также инсталляционными пакетами и патчами.
- **Операции**. Содержит различные операции, включая лицензирование приложений, просмотр и управление зашифрованными жесткими дисками и событиями шифрования.
- **Обнаружение устройств и развертывание**. Позволяет опрашивать сеть для обнаружения клиентских устройств и распределять устройства по группам администрирования вручную или автоматически. Этот раздел содержит мастер первоначальной настройки и мастер развертывания защиты.
- **Marketplace**. Содержит информацию о бизнес-решениях "Лаборатории Касперского", позволяет выбрать нужные вам и перейти к приобретению этих решений на сайте "Лаборатории Касперского".
- **Параметры**. Позволяет создавать резервную копию данных текущего состояния веб-плагина, чтобы впоследствии можно было восстановить сохраненное состояние. Содержит личные параметры, связанные с внешним видом интерфейса, такие как язык интерфейса или тема.

При необходимости вы можете свернуть главное меню до значков, нажав на значок стрелки (<<) внизу экрана.

Верхняя панель

Верхняя панель всегда отображается во всех разделах консоли и не может быть скрыта.

Левая часть панели содержит название и логотип приложения. Если вы нажмете на название или логотип приложения, откроется домашняя страница Kaspersky Security Center Web Console.

В правой части панели отображается следующее:

- Значок уведомления (🔔). Если нажать на значок, откроется панель с уведомлениями.
- Меню вашей учетной записи. Содержит ссылку на справку Kaspersky Security Center Linux. Также вы можете выйти из Kaspersky Security Center Linux, изменить пароль вашей учетной записи, просмотреть версию Kaspersky Security Center Web Console и список установленных веб-плагинов управления.

Рабочая область

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

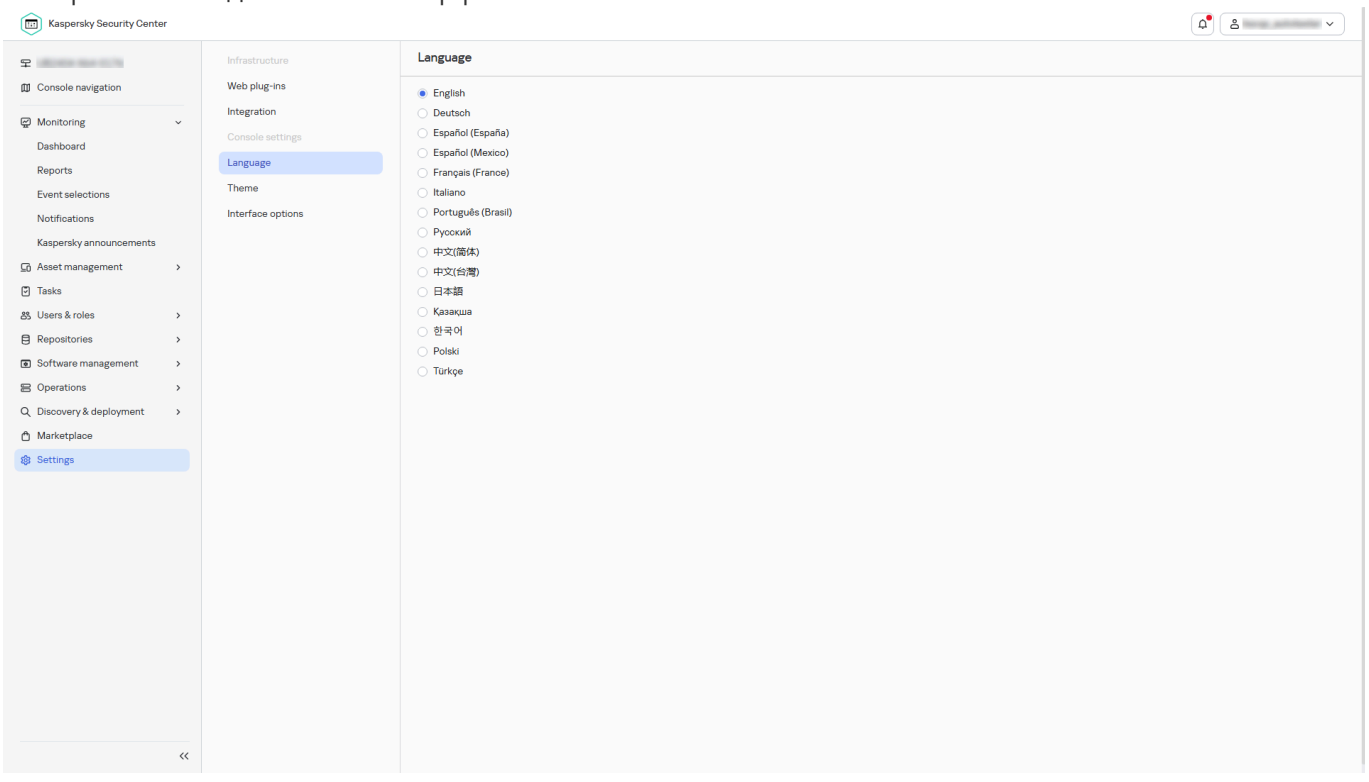
> Рекомендуется использовать одну вкладку браузера для работы с Kaspersky Security Center Web Console.

Изменение языка интерфейса Kaspersky Security Center Web Console

Вы можете выбрать один из поддерживаемых языков локализации в качестве языка интерфейса Kaspersky Security Center Web Console.

Чтобы изменить язык интерфейса:

1. В главном окне приложения перейдите в раздел **Параметры** → **Язык**.
2. Выберите необходимый язык интерфейса.



Изменение языка интерфейса Kaspersky Security Center Web Console

Изменение домашней страницы Kaspersky Security Center Web Console

Домашняя страница отображается после входа в Kaspersky Security Center Web Console.

По умолчанию раздел **Навигация консоли** установлен как домашняя страница. Если необходимо, вы можете изменить домашнюю страницу.

Чтобы изменить домашнюю страницу:

1. В разделе **Навигация консоли** наведите курсор мыши на элемент, который вы хотите установить в качестве домашней страницы.
2. После того как отобразится значок дома (), нажмите на этот значок.

   Домашняя страница изменена. На экране отобразится соответствующее сообщение. Элемент, выбранный в качестве домашней страницы, отмечен значком дома ().

Разделы **Marketplace** и **Параметры** невозможно установить в качестве домашней страницы.

Добавление и удаление закладок

Вы можете добавить часто используемые разделы Kaspersky Security Center Web Console в закладки, чтобы быстро получать к ним доступ из раздела **Закладки** в главном меню.

Если вы не добавили ни одного раздела в закладки, раздел **Закладки** не отображается в главном меню.

Вы можете добавить в закладки только те разделы, которые отображают страницы. Например, если вы перейдете в раздел **Управление активами** → **Управляемые устройства**, откроется страница с таблицей устройств, что означает, что вы можете добавить этот раздел в закладки. Если после выбора раздела в главном меню не отображается окно или элемент, то добавить такой раздел в закладки невозможно.

Чтобы добавить раздел в закладки:

1. В главном меню наведите курсор мыши на раздел, который вы хотите закрепить.
2. После того как значок закладки () отобразится, нажмите на значок.

   Раздел отображается в разделе **Закладки**.

Чтобы удалить раздел из закладок:

1. В главном окне приложения перейдите в раздел **Закладки**.
2. Наведите курсор мыши на раздел, который вы хотите удалить из закладок, и нажмите на значок закладки ( ).

   Раздел удален из закладок.

Вы также можете добавлять и удалять разделы из закладок в разделе **Навигация консоли**, наведя на них курсор мыши и нажав на значок закладки (). Выбранный элемент будет отмечен значком закладки () и отобразится в разделе **Закладки** главного меню. Если вы хотите удалить элемент из закладок, нажмите на значок закладки ().

Раздел **Закладки** отображается только в главном меню. Этот раздел никогда не отображается на странице **Навигация консоли**.

Удаление Kaspersky Security Center Web Console

Вам может потребоваться удалить Сервер Kaspersky Security Center Web Console (даже также Kaspersky Security Center Web Console) в следующих случаях:

- Для восстановления данных из резервной копии с помощью другого общего сертификата.
- Для перевыпуска общего сертификата Сервера администрирования.
- Для замены сертификата Web Console пользовательским сертификатом.
- Если Kaspersky Security Center Web Console больше не используется на устройстве.

Чтобы удалить Kaspersky Security Center Web Console:

1. В зависимости от вашего дистрибутива Linux выполните одну из следующих команд:
   - `sudo dnf remove ksc-web-console`
   - `sudo apt remove ksc-web-console`
2. Проверьте результат, выполнив следующую команду:

   `sudo systemctl status KSC*`

   Kaspersky Security Center Web Console должен отсутствовать в выходных данных команды.

Если вы хотите восстановить Kaspersky Security Center Web Console, установите его на устройство, как описано в статье Установка Kaspersky Security Center Web Console.

Мастер первоначальной настройки

Приложение 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 приложение следующие изменения:

- Добавить файлы ключей или ввести коды активации, которые можно автоматически распространять на устройства в группах администрирования.
- Настроить рассылку уведомлений о событиях, происходящих в процессе работы Сервера администрирования и управляемых приложений по электронной почте.

- Сформировать политику защиты рабочих станций и серверов, а также задачи поиска вредоносного ПО, получения обновлений и резервного копирования данных для верхнего уровня иерархии управляемых устройств.

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

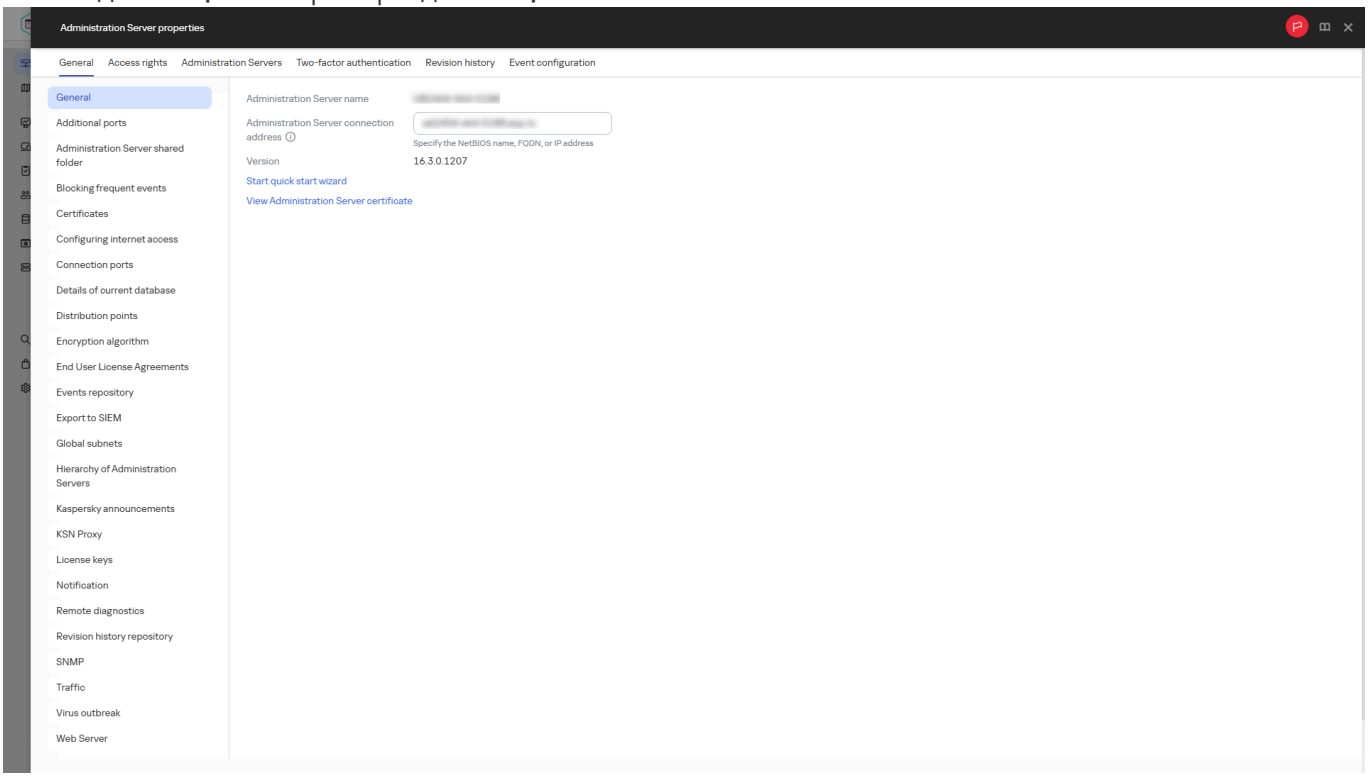
Приложение автоматически предлагает запустить мастер первоначальной настройки после установки Сервера администрирования при первом подключении к Серверу. Вы также можете запустить мастер первоначальной настройки вручную в любое время.

Чтобы запустить мастер первоначальной настройки вручную:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Общие**.



Окно свойств Сервера администрирования

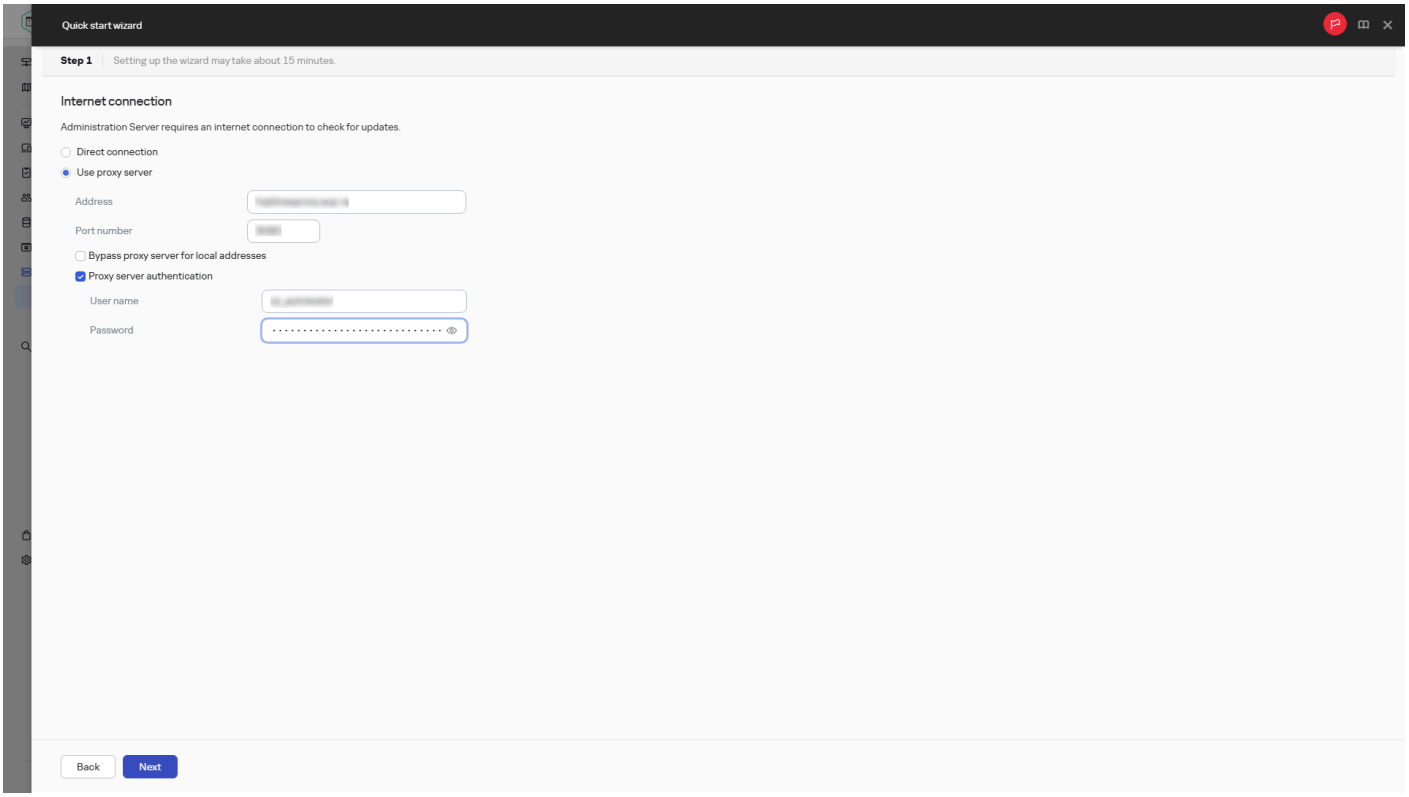
3. Нажмите на кнопку **Запустить мастер первоначальной настройки**.

   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

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 приложений "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:



Параметры подключения к интернету

- **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**

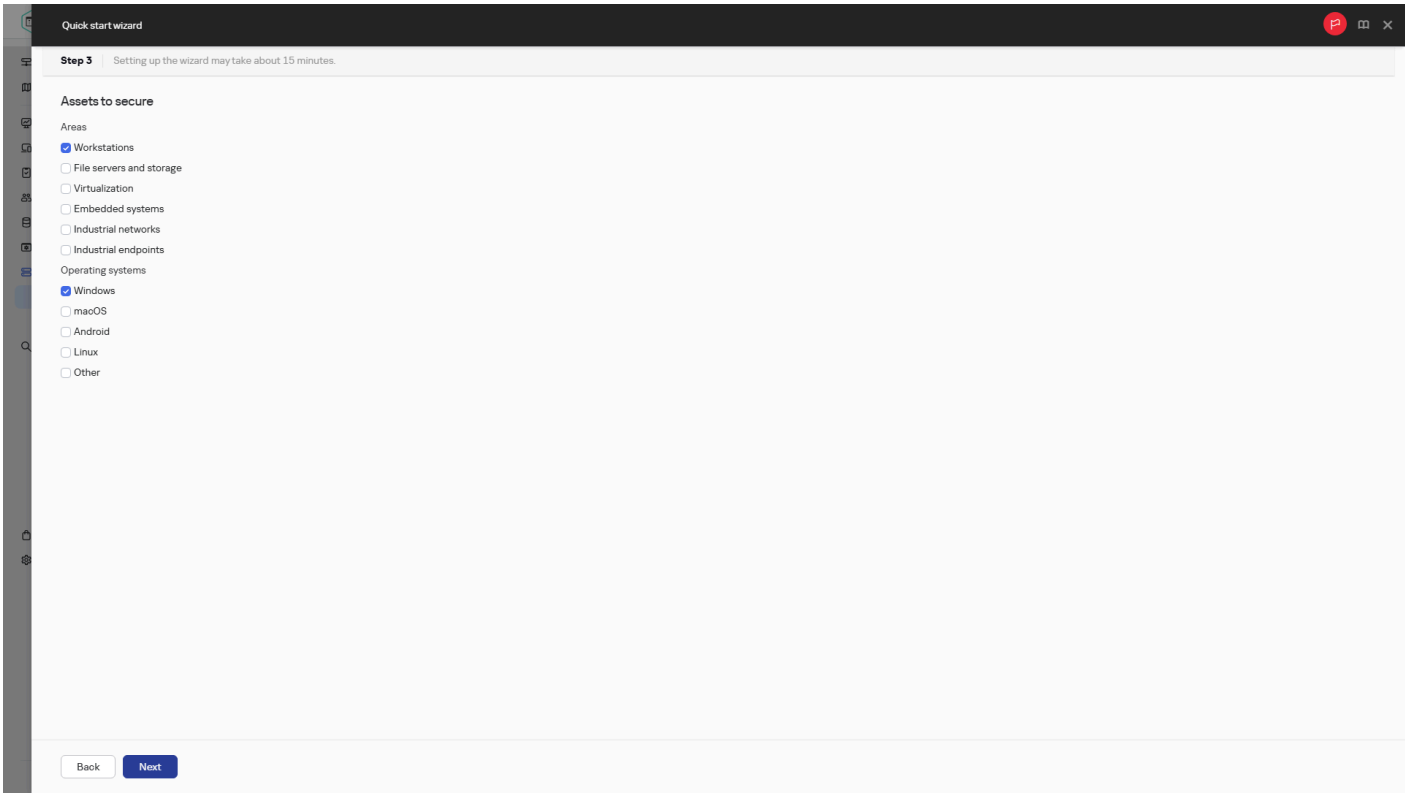
  Пароль пользователя, с помощью учетной записи которого выполняется подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

  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. Загрузка требуемых обновлений

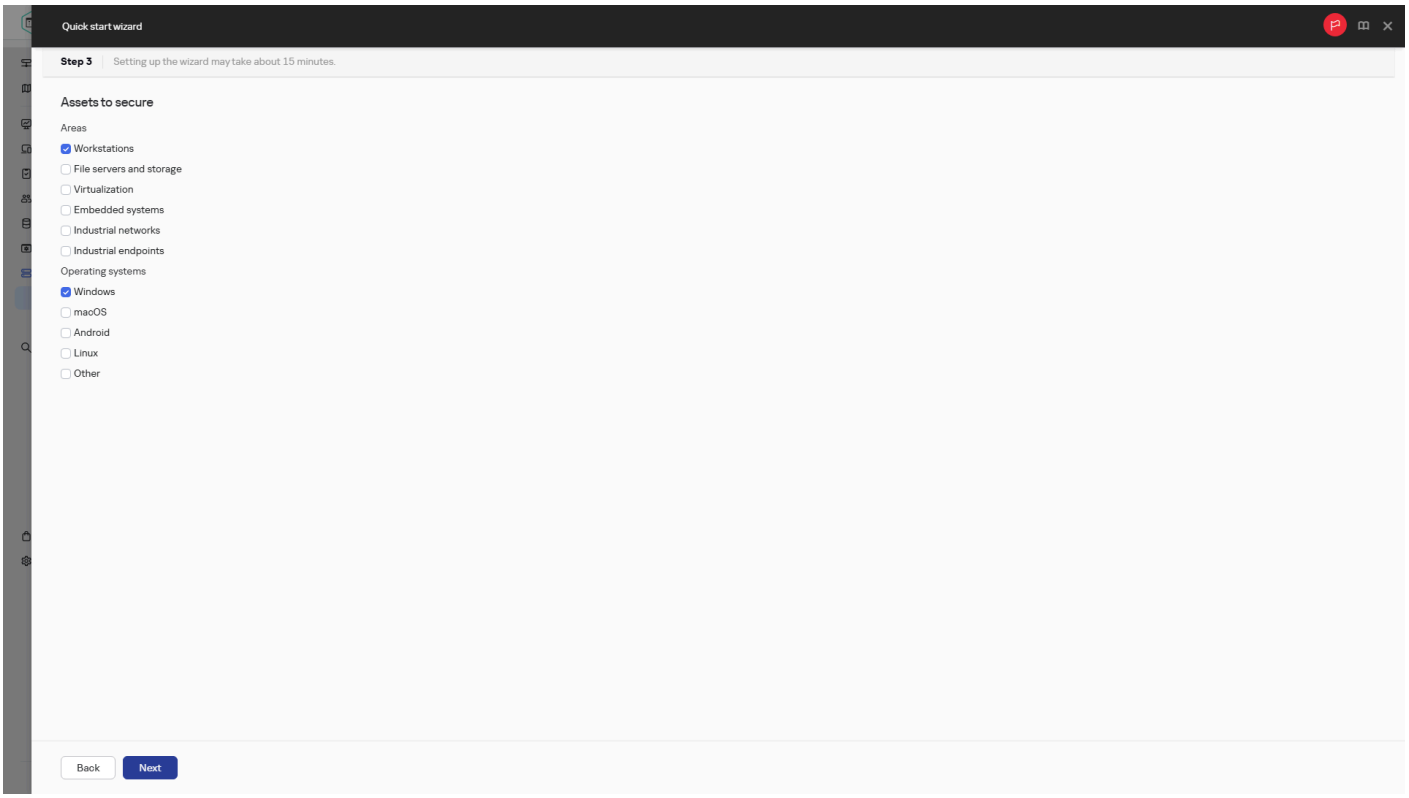
Необходимые обновления загружаются с серверов "Лаборатории Касперского" автоматически.



Загрузка требуемых обновлений

Шаг 3. Выбор активов для защиты

Выберите области защиты и операционные системы, которые используются в вашей сети. При выборе этих параметров вы указываете фильтры для плагинов управления приложениями и дистрибутивов на серверах "Лаборатории Касперского", которые вы можете загрузить для установки на клиентские устройства в вашей сети.



Выбор активов для защиты

Выберите следующие параметры:

- **Области**

  Вы можете выбрать одну из следующих областей защиты:

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

- **Операционные системы**

  Вы можете выбрать одну из следующих платформ:

  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - Другое

  Дополнительные сведения о поддерживаемых версиях операционных систем см. в разделе Аппаратные и программные требования Kaspersky Security Center Web Console.

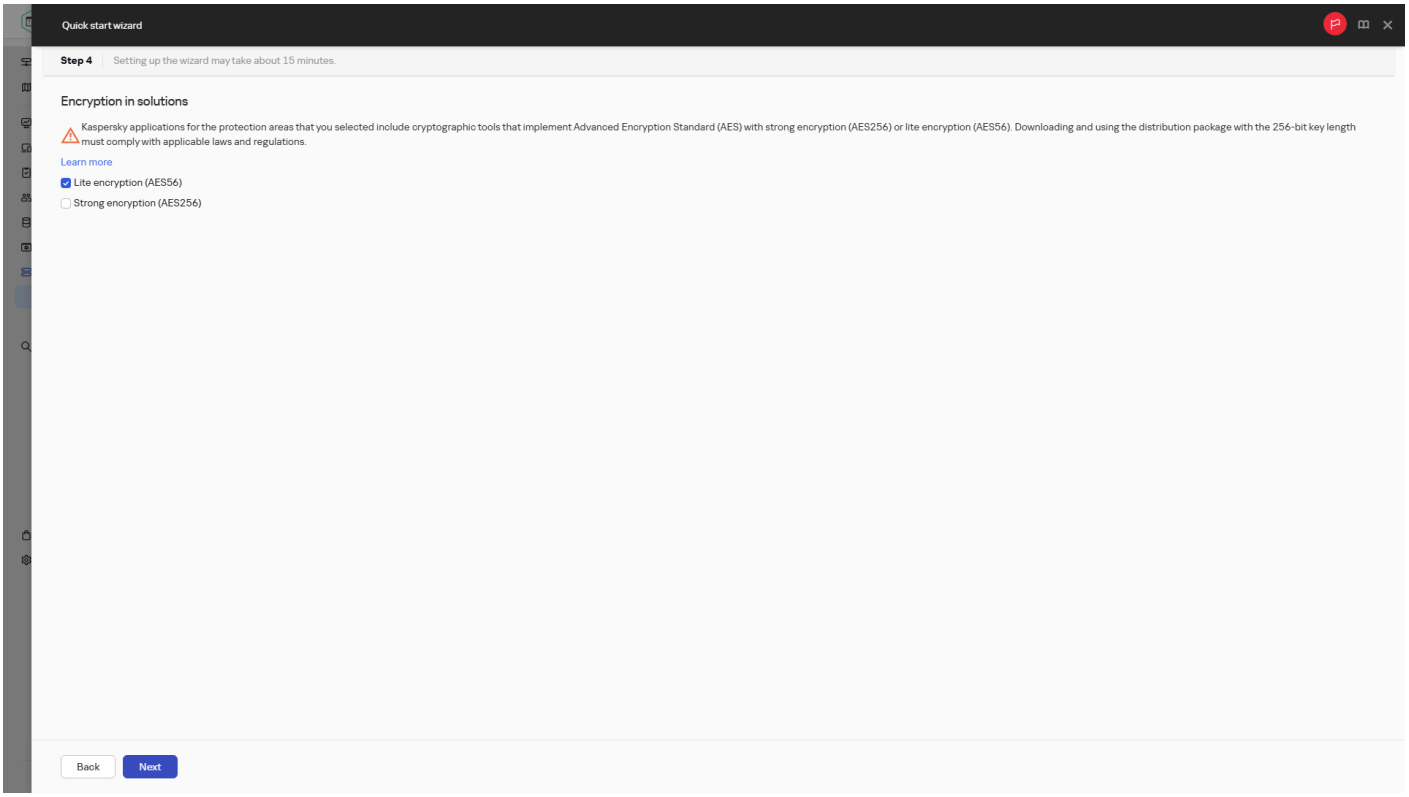
Можно выбрать инсталляционные пакеты приложений "Лаборатории Касперского" из списка доступных инсталляционных пакетов позднее без запуска мастера первоначальной настройки. Для упрощения поиска необходимых инсталляционных пакетов вы можете фильтровать список доступных инсталляционных пакетов различным критериям.

Шаг 4. Выбор шифрования

Окно **Шифрование** отображается, только если в качестве области защиты выбран вариант **Рабочие станции**.

Kaspersky Endpoint Security для Windows включает инструменты шифрования информации, хранящейся на клиентских устройствах в операционной системой Windows. Эти инструменты шифрования имеют расширенный стандарт шифрования (AES), реализованный с длиной ключа 256 бит или 56 бит.

Загрузка и использование дистрибутива с длиной ключа 256 бит должна выполняться в соответствии с действующими законами и правилами. Чтобы загрузить дистрибутив Kaspersky Endpoint Security для Windows, действительный для нужд вашей организации, обратитесь к законодательству страны, в которой расположены клиентские устройства вашей организации.



Выбор шифрования

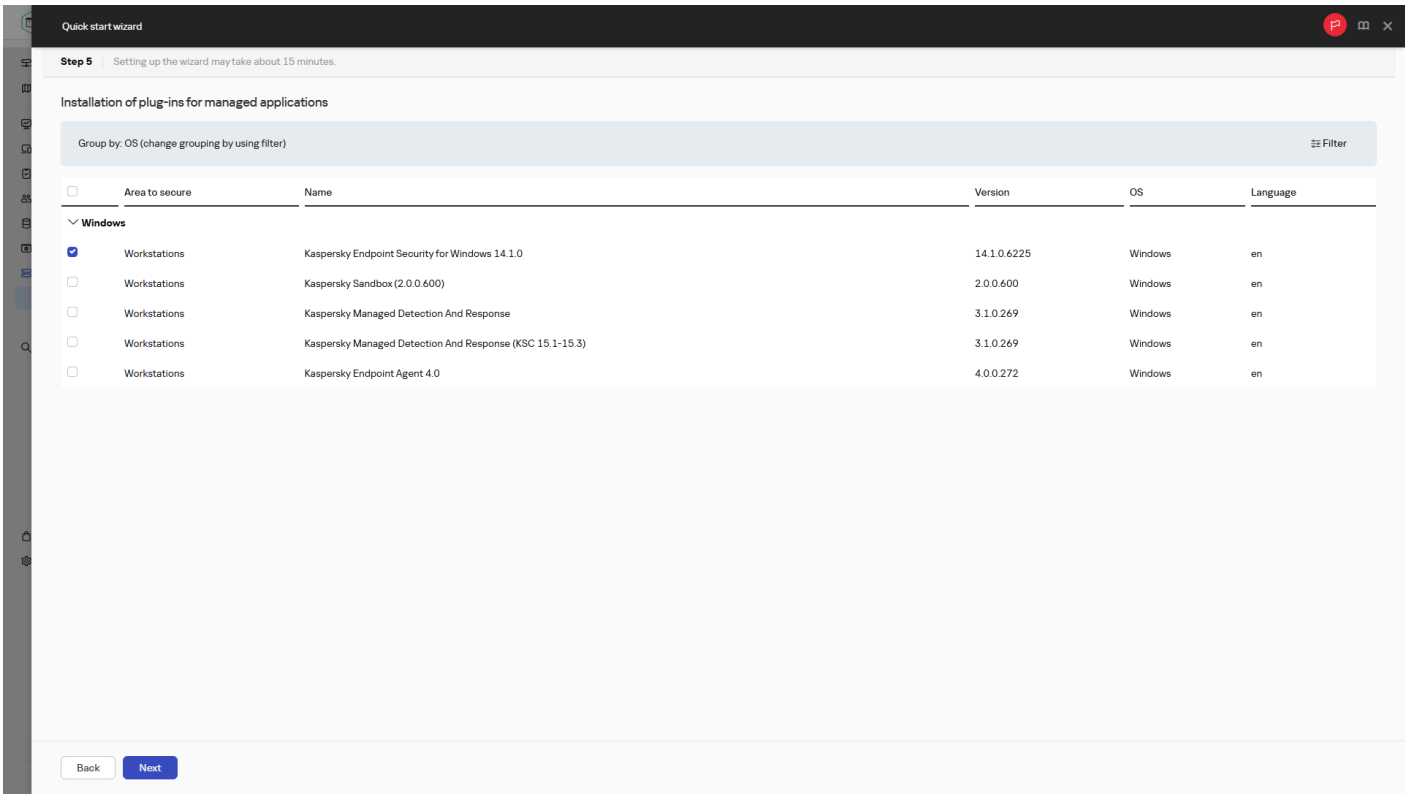
В окне **Шифрование** выберите один из следующих типов шифрования:

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

Вы можете выбрать дистрибутив для Kaspersky Endpoint Security для Windows с необходимым типом шифрования позднее без запуска мастера первоначальной настройки.

Шаг 5. Настройка установки плагинов для управляемых приложений

Выберите плагины для управляемых приложений для установки. Отображается список плагинов, расположенных на серверах "Лаборатории Касперского". Список отфильтрован в соответствии с параметрами, выбранными на предыдущем шаге мастера. По умолчанию в полный список включены плагины всех языков. Чтобы отображался только плагин на выбранном языке, используйте фильтр.



Установка плагинов для управляемых приложений

Список плагинов включает в себя следующие столбцы:

- **Область защиты**

  В этом столбце отображаются выбранные области для защиты.

- **Тип**

  В этом столбце отображаются типы плагинов.

- **Имя**

  Выбраны плагины в зависимости от областей защиты и платформ, выбранных на предыдущем шаге.

- **Версия**

  В список включены плагины всех версий, размещенных на серверах "Лаборатории Касперского". По умолчанию выбраны плагины последних версий.

- **Последняя версия**

  В этом столбце указано, является ли версия плагина последней. Если отображается значение **true**, соответствующий плагин имеет последнюю версию. Если отображается значение **false**, для соответствующего плагина существует более поздняя версия.

- **ОС**

  В этом столбце отображаются плагины операционных систем.

- **Язык**

  По умолчанию язык локализации плагина зависит от языка Kaspersky Security Center Linux, который вы выбрали при установке. Другие языки можно выбрать в раскрывающемся списке **Отображать язык Консоли администрирования или**.

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

Вы можете установить плагины управления для приложений "Лаборатории Касперского" вручную позднее без запуска мастера первоначальной настройки.

Мастер первоначальной настройки автоматически установит выбранные плагины. Для установки некоторых плагинов вам нужно принять условия Лицензионного соглашения. Ознакомьтесь с текстом Лицензионного соглашения, который отображается на экране, установите флажок **Я принимаю условия использования Kaspersky Security Network** и нажмите на кнопку **Установить**. Если вы не согласны с условиями Лицензионного соглашения, плагин не установится.

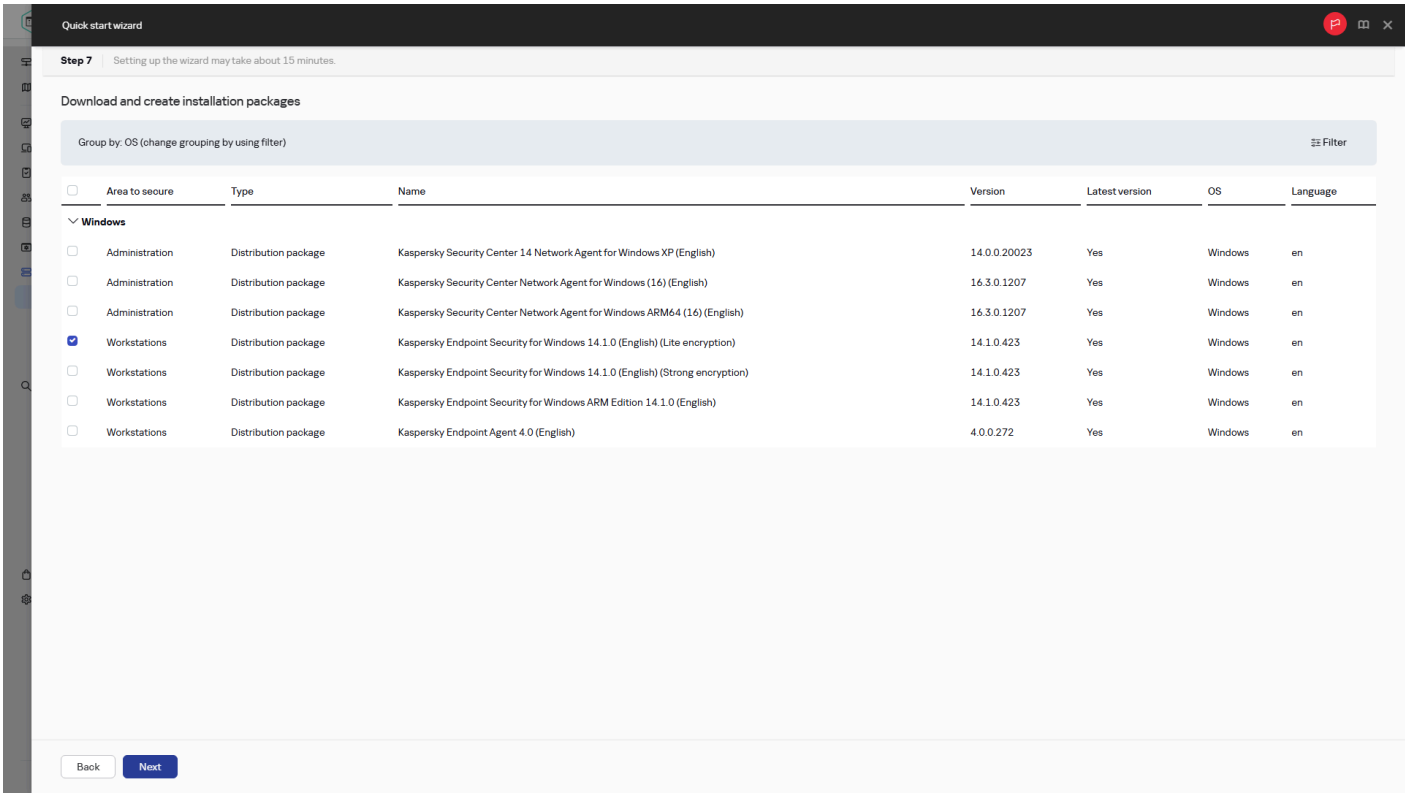
Когда все выбранные плагины будут установлены, мастер первоначальной настройки автоматически перейдет к следующему шагу.

Шаг 6. Загрузка дистрибутивов и создание инсталляционных пакетов

Выберите дистрибутив для загрузки.

> Для дистрибутивов управляемых приложений может потребоваться установка определенной минимальной версии Kaspersky Security Center Linux.

После того, как вы выбрали тип шифрования для Kaspersky Endpoint Security для Windows, отобразится список дистрибутивов для обоих типов шифрования. В списке выбран дистрибутив с выбранным типом шифрования. Вы можете выбрать дистрибутив для любого типа шифрования. Язык дистрибутива соответствует языку Kaspersky Security Center Linux. Если дистрибутив приложения для языка Kaspersky Security Center Linux отсутствует, выбирается дистрибутив на английском языке.



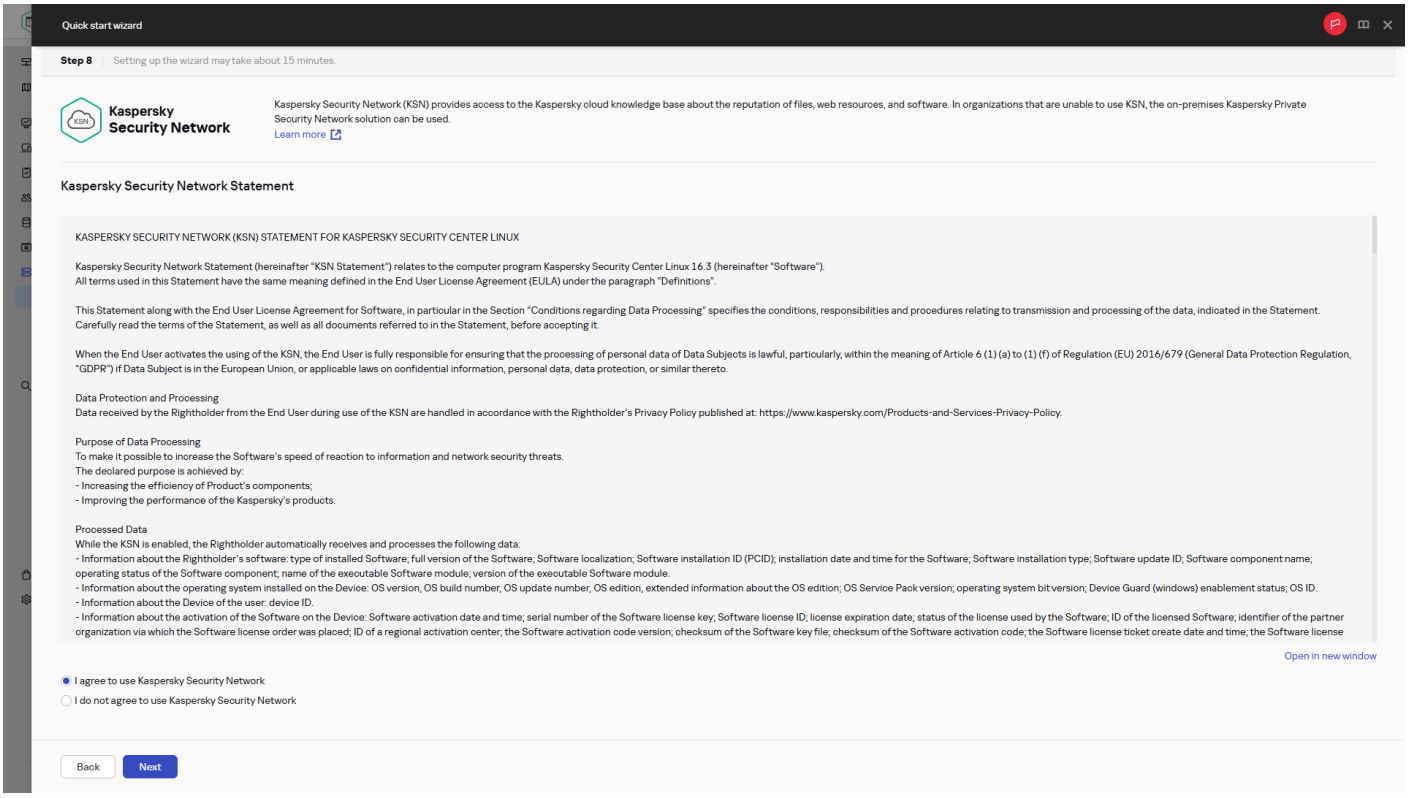
Загрузка дистрибутивов и создание инсталляционных пакетов

Чтобы завершить загрузку некоторых дистрибутивов вам нужно принять Лицензионное соглашение. При нажатии кнопки **Принять** отображается текст Лицензионного соглашения. Чтобы перейти к следующему шагу мастера, вам нужно принять положения и условия Лицензионного соглашения, а также условия Политики конфиденциальности "Лаборатории Касперского". Если вы не принимаете положения и условия, загрузка пакета отменяется.

После того, как вы приняли положения и условия Лицензионного соглашения, а также условия Политики конфиденциальности "Лаборатории Касперского", загрузка дистрибутивов продолжается. В дальнейшем инсталляционные пакеты можно использовать для развертывания приложений "Лаборатории Касперского" на клиентских устройствах.

Шаг 7. Настройка Kaspersky Security Network

Настройте параметры передачи информации о работе Kaspersky Security Center Linux в базу знаний Kaspersky Security Network.



Настройка Kaspersky Security Network

Выберите один из следующих вариантов:

- **Я принимаю условия использования Kaspersky Security Network**

  Kaspersky Security Center Linux и управляемые приложения, установленные на клиентских устройствах, в автоматическом режиме будут предоставлять информацию об их работе Kaspersky Security Network. Сотрудничество с Kaspersky Security Network обеспечивает более быстрое обновление баз данных о вирусах и угрозах, что увеличивает скорость реагирования на возникающие угрозы безопасности.

- **Я не принимаю условия использования Kaspersky Security Network**

  Kaspersky Security Center Linux и управляемые приложения не будут предоставлять информацию о своей работе Kaspersky Security Network.

  Если вы выбрали этот параметр, использование Kaspersky Security Network будет выключено.

Вы можете настроить доступ к Kaspersky Security Network (KSN) позднее без запуска мастера первоначальной настройки.

Шаг 8. Выбор способа активации приложения

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

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

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

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

- **Укажите файл ключа**

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

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

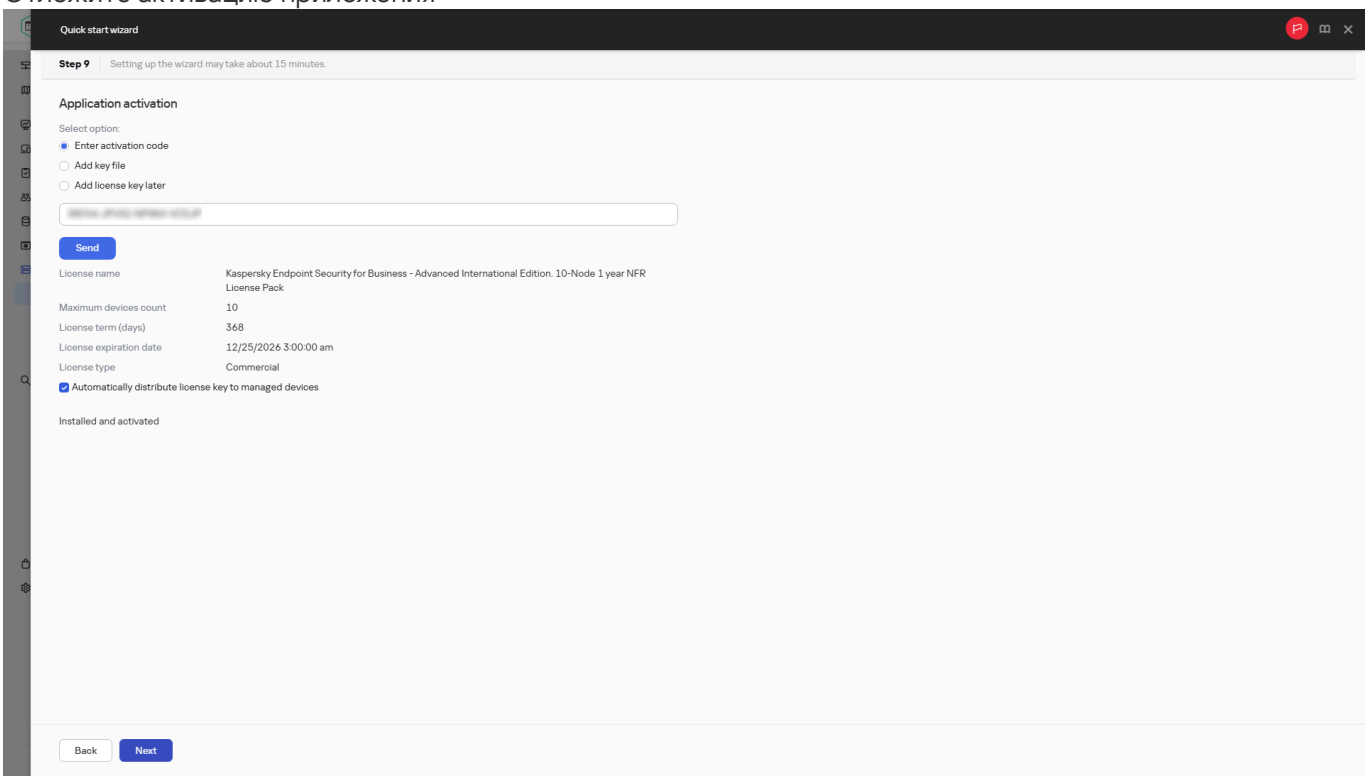
  Чтобы активировать приложение с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

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

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

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

- Отложите активацию приложения



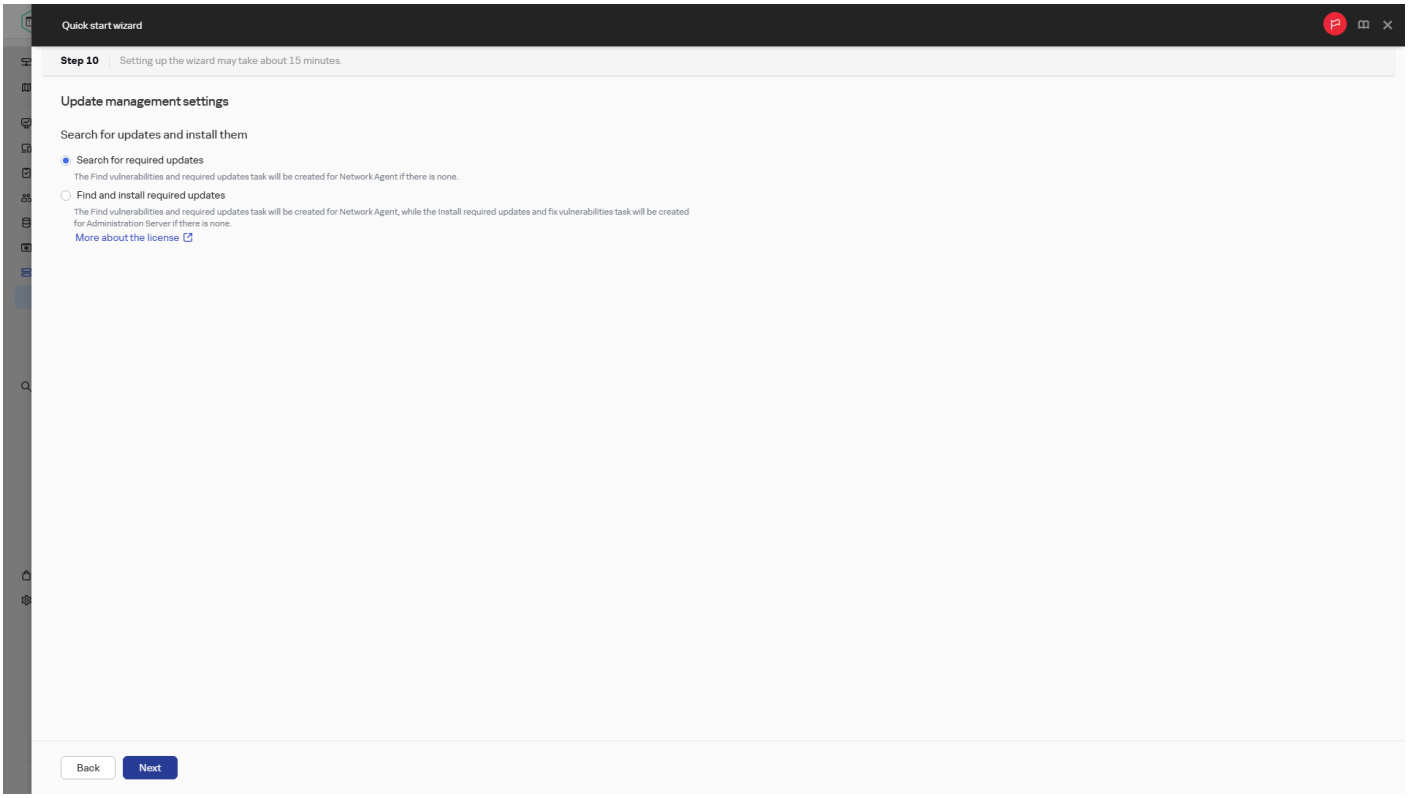
Выбор способа активации приложения

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

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

Шаг 9. Указание параметров управления обновлениями приложений сторонних производителей

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



Управление параметрами обновлений приложений сторонних приложений

Для обновлений приложений сторонних производителей выберите один из следующих вариантов:

- **Искать требуемые обновления**

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

  По умолчанию этот вариант выбран.

- **Искать и устанавливать требующиеся обновления**

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

  Этот параметр доступен при наличии лицензии на Системное администрирование.

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

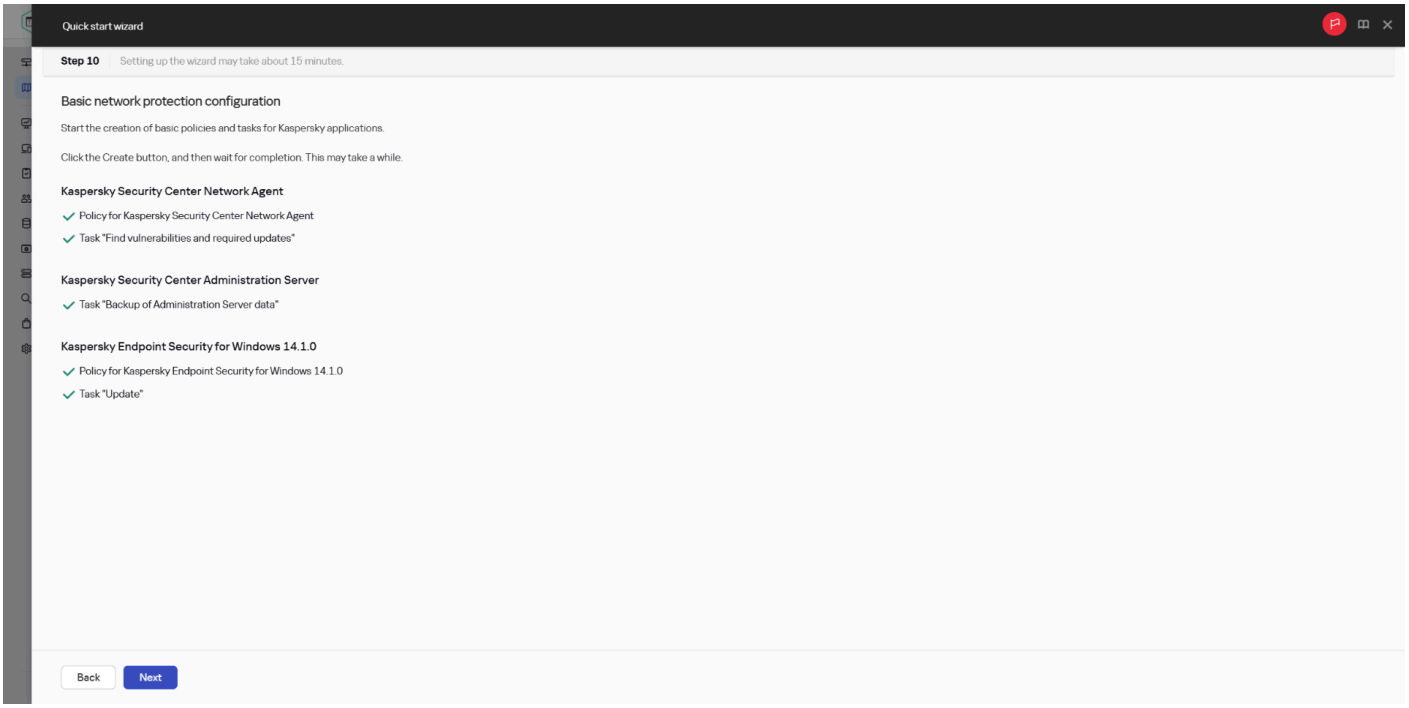
Обновления Центра обновления Windows загружаются на клиентские устройства в соответствии с параметрами политики домена. Политика Агента администрирования создается автоматически, если она не была создана ранее.

Вы можете создать задачи *Поиск уязвимостей и требуемых обновлений* и *Установка требуемых обновлений и закрытие уязвимостей* позднее без запуска мастера первоначальной настройки.

Шаг 10. Создание базовой конфигурации защиты сети

Вы можете проверить список созданных политик и задач.

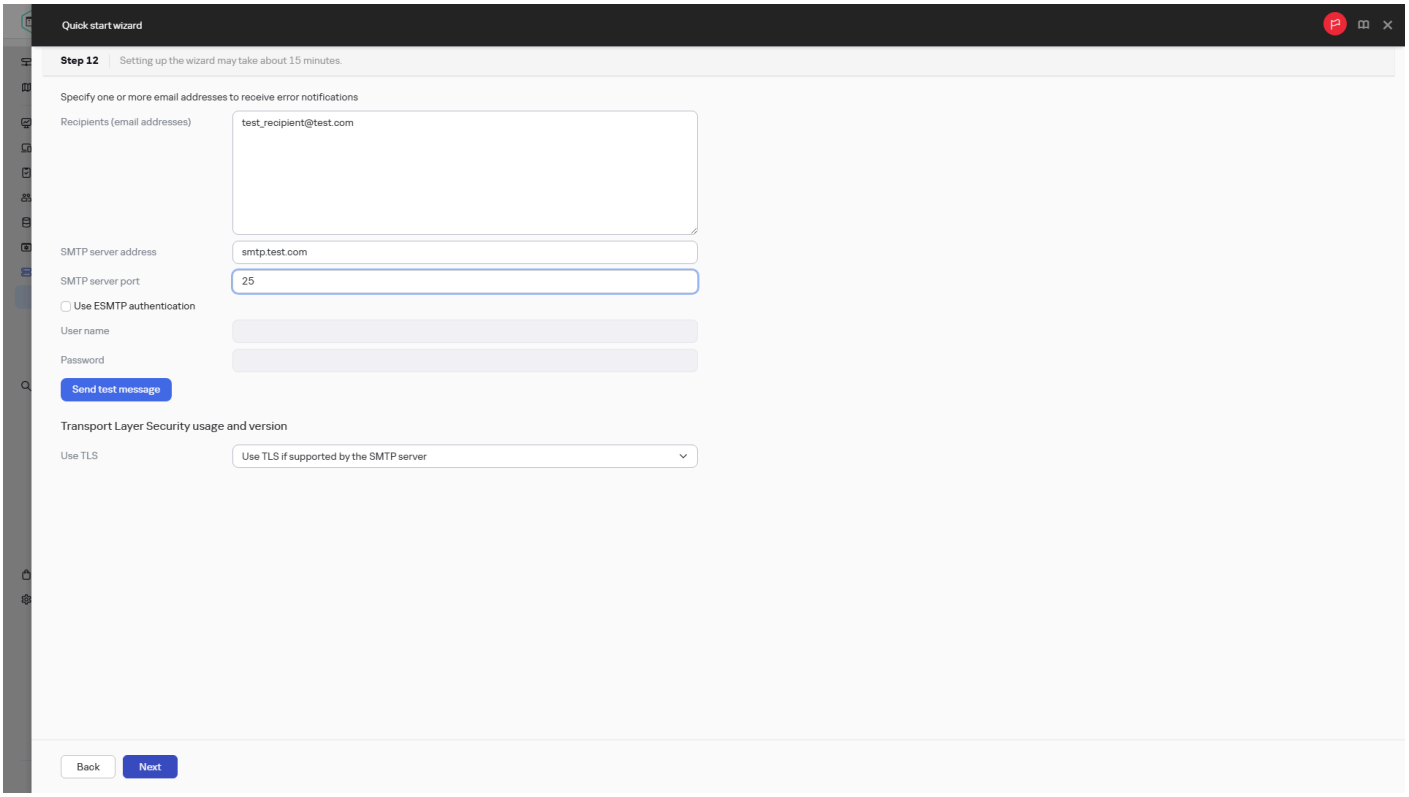
Для перехода на следующий шаг мастера дождитесь окончания создания политик и задач.



Создание базовой конфигурации защиты сети

Шаг 11. Настройка параметров отправки уведомлений по электронной почте

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



Настройка параметров отправки уведомлений по электронной почте

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

- **Получатели (адреса электронной почты)**

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

- **Адрес SMTP-сервера**

  Адрес или адреса почтовых серверов вашей организации.

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

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

- **Порт SMTP-сервера**

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

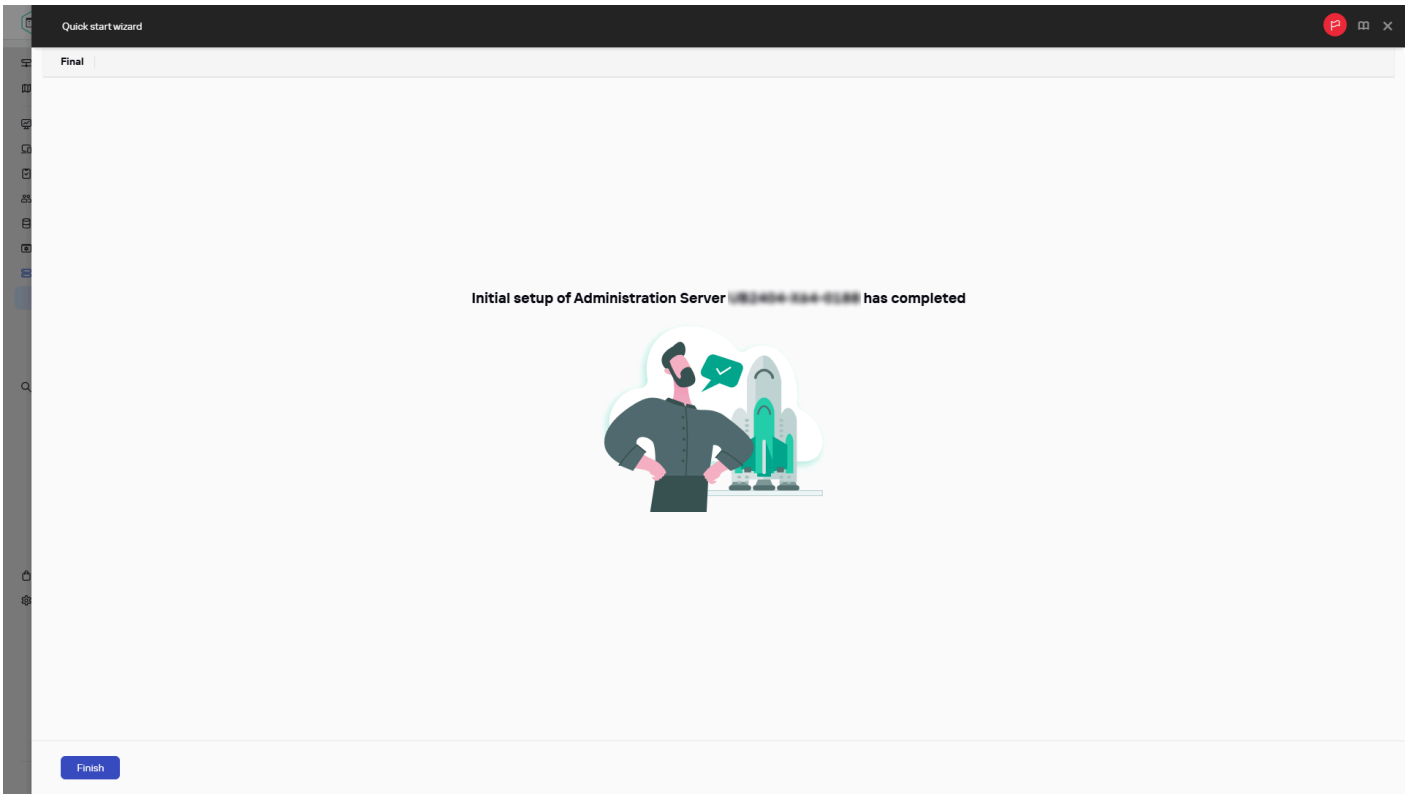
- **Использовать ESMTP-аутентификацию**

  Включение поддержки ESMTP-аутентификации. После установки флажка 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 12. Завершение работы мастера первоначальной настройки

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



Последний шаг мастера первоначальной настройки

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

Мастер развертывания защиты

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

Мастер развертывания защиты выполнит следующие действия:

- Загружает инсталляционный пакет для установки приложения (если он не был создан раньше). Инсталляционный пакет находится в разделе **Управление программным обеспечением** → **Инсталляционные пакеты**. Вы можете использовать этот инсталляционный пакет для установки приложения в дальнейшем.

- Создает и запускает задачу удаленной установки для набора устройств или для группы администрирования. Созданная задача удаленной установки хранится в разделе **Задачи**. Вы можете запустить эту задачу в дальнейшем вручную. Тип задачи – **Удаленная установка приложения**.

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

Шаг 1. Запуск мастера развертывания защиты

Мастер развертывания защиты можно запустить вручную.

Чтобы запустить мастер развертывания защиты вручную,

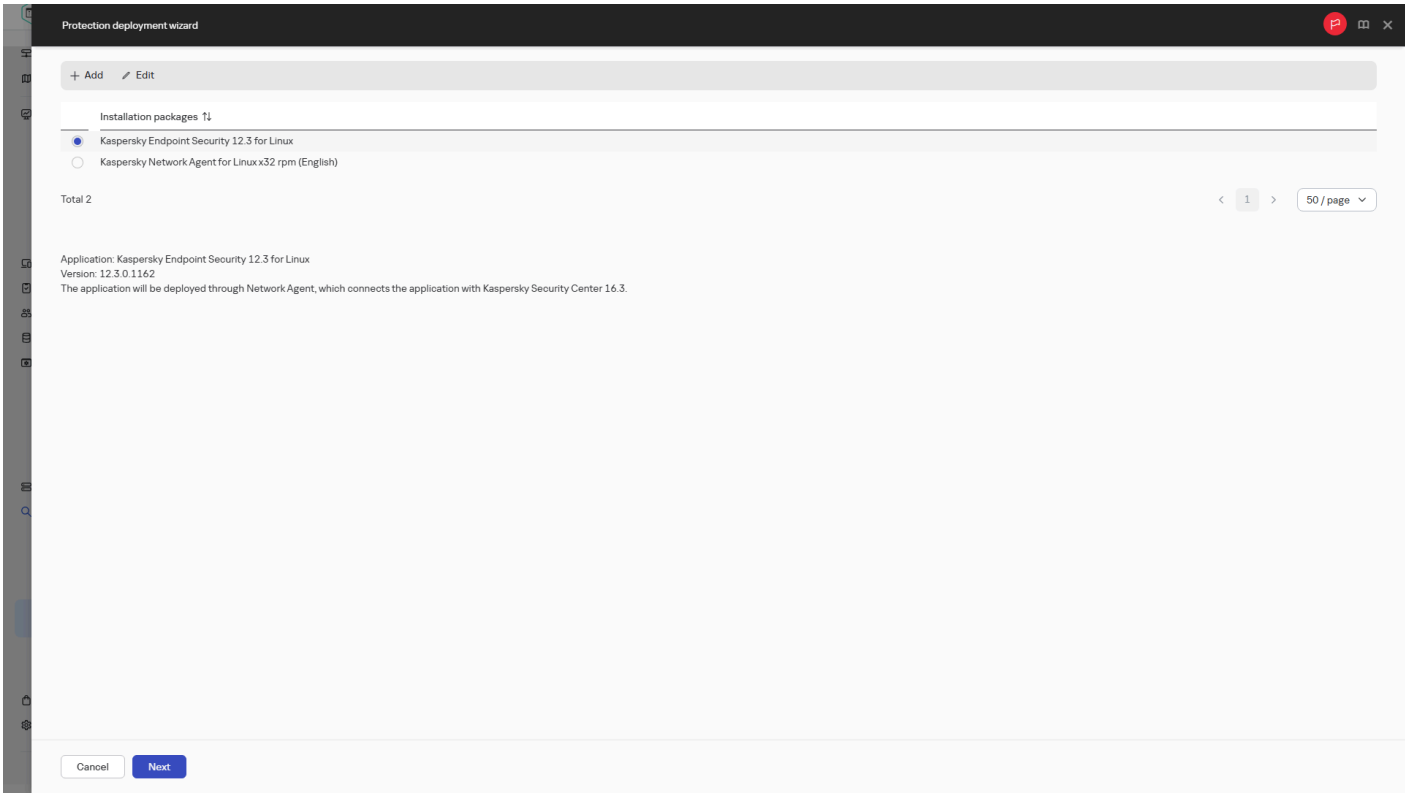
В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Мастер развертывания защиты**.

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

Шаг 2. Выбор инсталляционного пакета

Выберите инсталляционный пакет приложения, которое требуется установить.

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



Выбор инсталляционного пакета

Шаг 3. Выбор способа распространения файла ключа или кода активации

Выберите способ распространения файла ключа или кода активации:

- **Не добавлять лицензионный ключ в инсталляционный пакет**

  Если выбран этот вариант, ключ будет автоматически распространяться на те устройства, для которых он подходит:

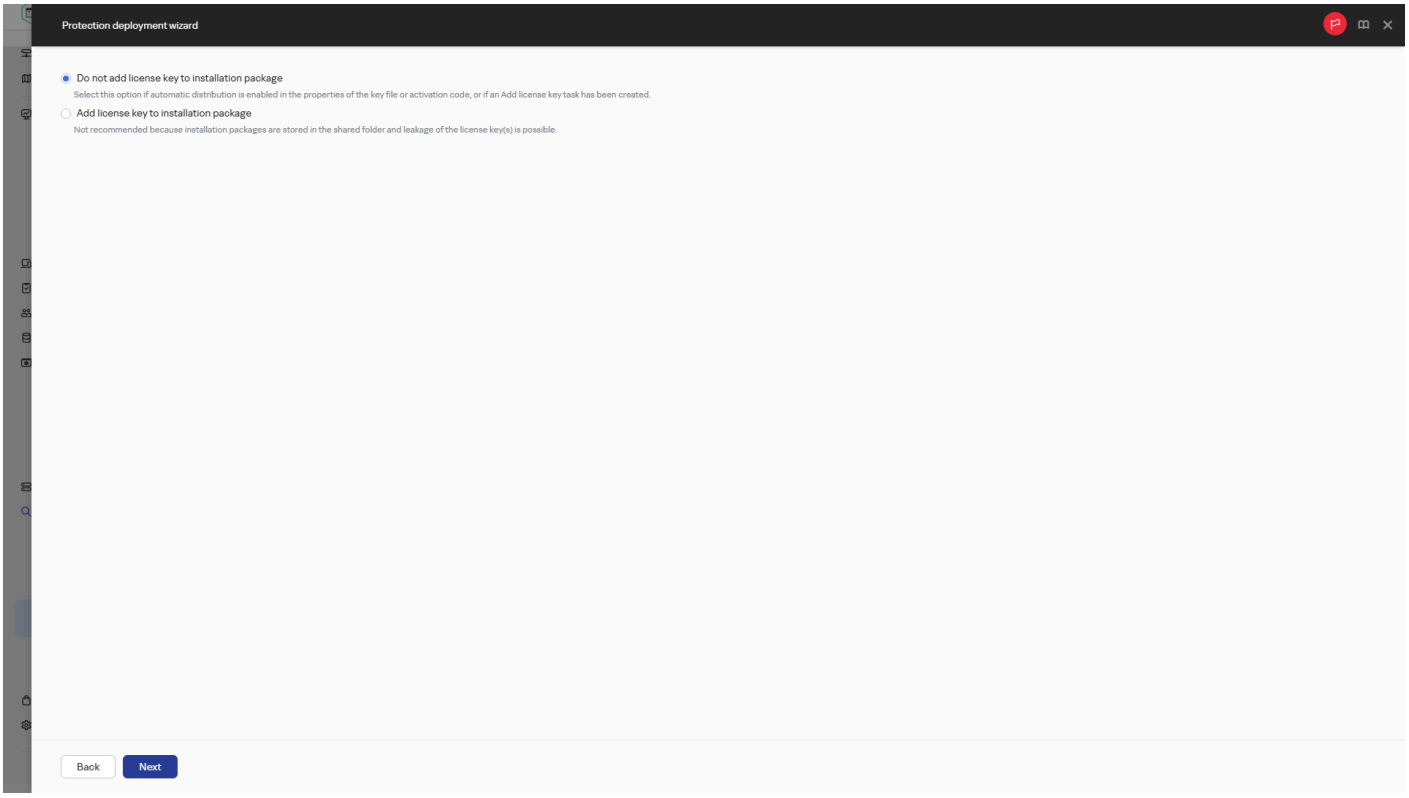
  - если в свойствах ключа настроено автоматическое распространение;
  - если создана задача **Добавление ключа**.

- **Добавить лицензионный ключ в инсталляционный пакет**

  Ключ распространяется на устройства вместе с инсталляционным пакетом.

  > Не рекомендуется распространять ключ таким способом, так как по умолчанию к хранилищу инсталляционных пакетов настроен общий доступ на чтение.

Если инсталляционный пакет уже содержит файл ключа или код активации, это окно отображается, но оно содержит только информацию о лицензионном ключе.

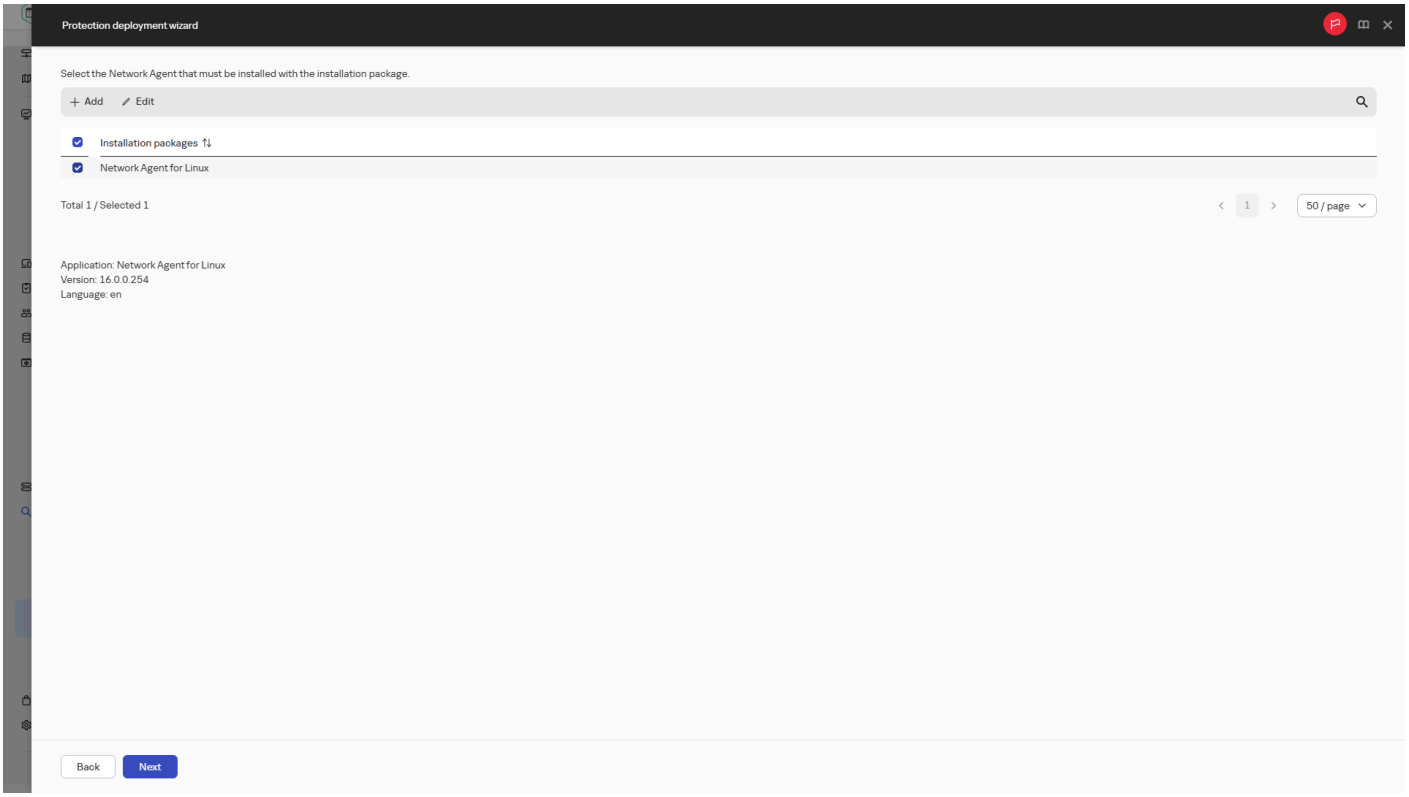


Выбор способа распространения файла ключа или кода активации

Шаг 4. Выбор версии Агента администрирования

Если вы выбрали инсталляционный пакет приложения, отличный от Агента администрирования, необходимо также установить Агент администрирования для подключения приложения к Серверу администрирования.

Выберите последнюю версию Агента администрирования.



Выбор версии Агента администрирования

Шаг 5. Выбор устройств

Укажите список устройств, на которые требуется установить приложение:

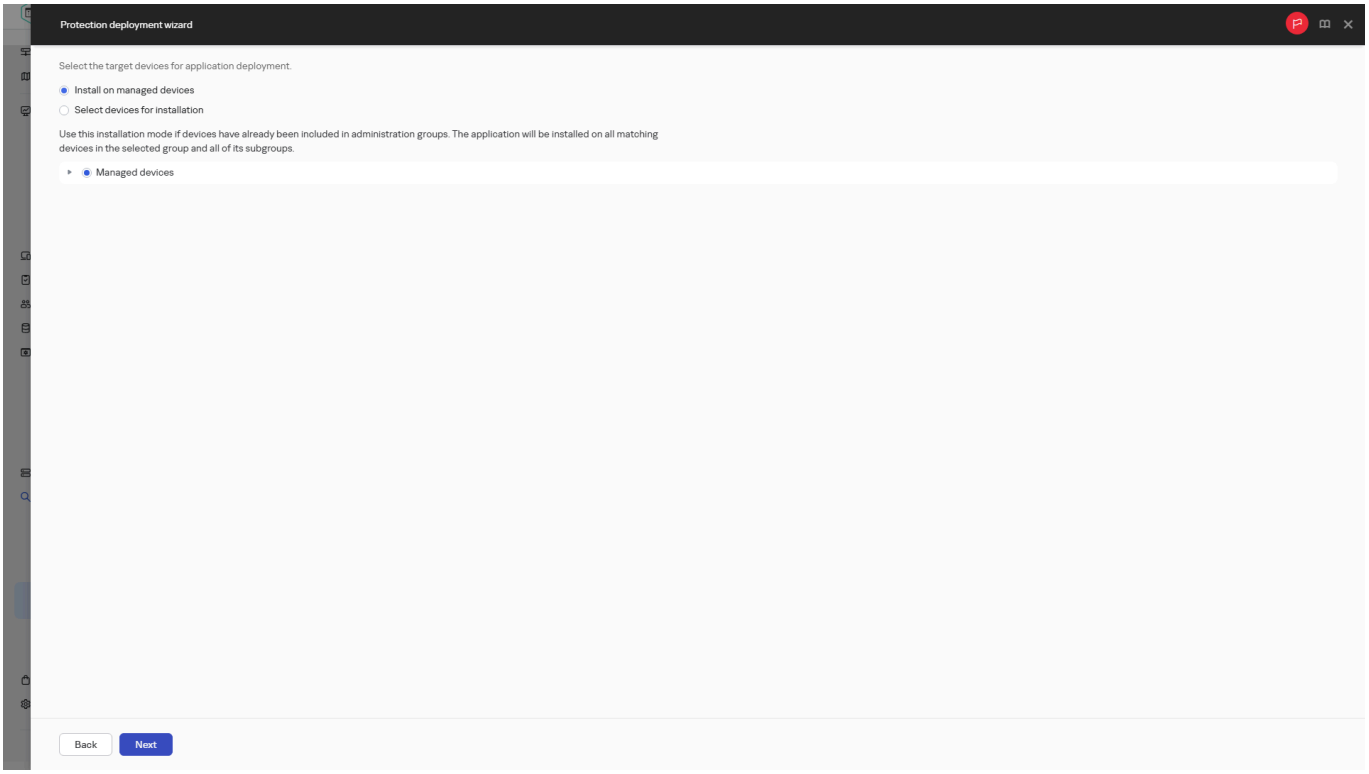
- **Установить на управляемые устройства**

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

- **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.



Указание устройств, на которые будет установлено приложение

Шаг 6. Задание параметров задачи удаленной установки

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

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

- **С помощью Агента администрирования**

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

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

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

  По умолчанию параметр включен.

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

  Если флажок установлен, инсталляционные пакеты передаются на клиентские устройства средствами операционной системы через агенты обновлений. Этот вариант можно выбрать, если в сети есть хотя бы один агент обновлений.

  Если установлен флажок **С помощью Агента администрирования**, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

По умолчанию флажок установлен для задач удаленной установки, созданных на виртуальном Сервере администрирования.

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

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

- **Средствами операционной системы с помощью Сервера администрирования**

  Если этот параметр включен, доставка файлов на клиентские устройства будет осуществляться средствами операционной системы клиентских устройств с помощью Сервера администрирования. Этот параметр можно включить, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

  По умолчанию параметр включен.

Настройте дополнительный параметр:

- **Не устанавливать приложение, если оно уже установлено**

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

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

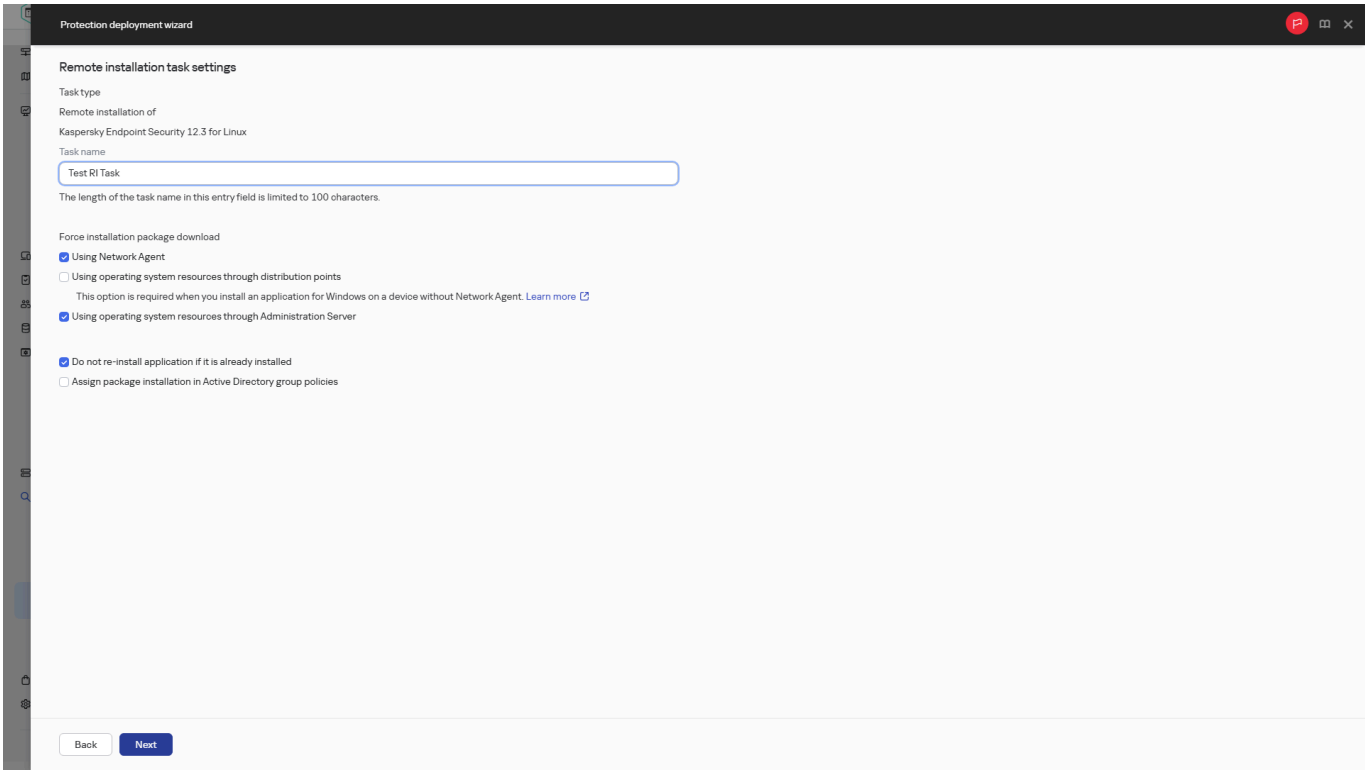
  По умолчанию параметр включен.

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

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

  Параметр доступен, если выбран инсталляционный пакет Агента администрирования.

По умолчанию параметр выключен.



Задание параметров задачи удаленной установки

Шаг 7. Управление перезагрузкой

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

- **Не перезагружать устройство**

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

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

По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

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

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

  Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

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

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

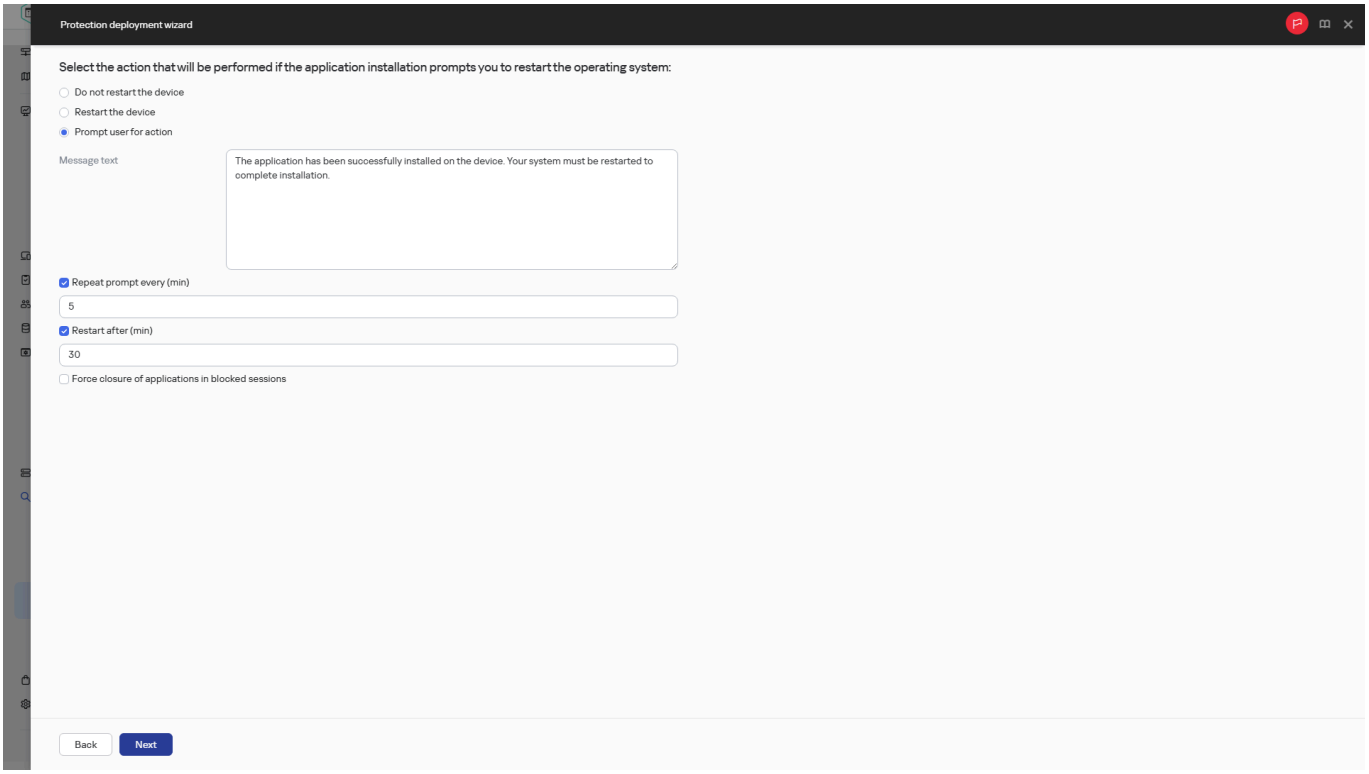
- **Принудительно закрывать приложения в заблокированных сеансах**

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

  Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.



Указание параметра перезагрузки операционной системы

Шаг 8. Удаление несовместимых приложений перед установкой

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

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

Отображается список несовместимых приложений.

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

Шаг 9. Перемещение устройств в папку Управляемые устройства

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

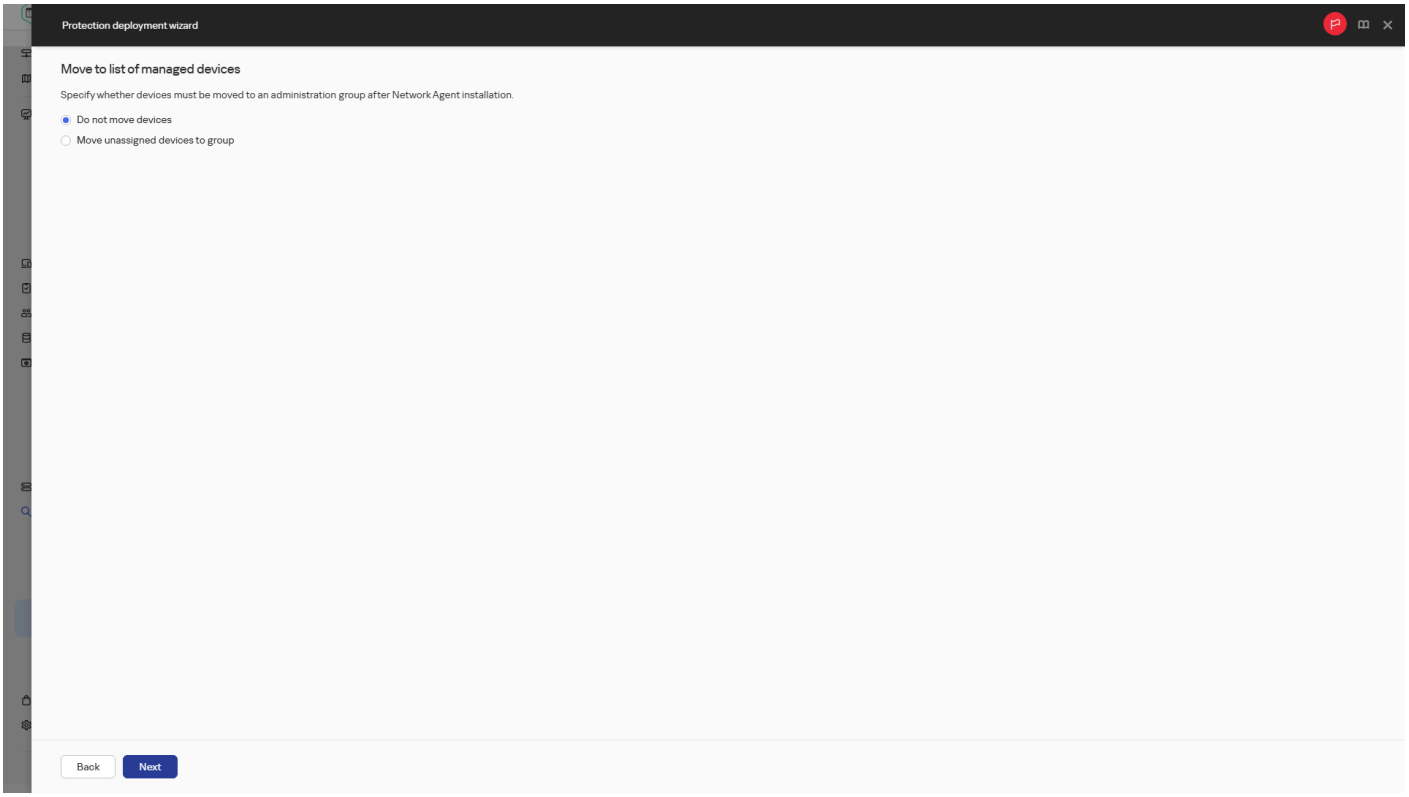
- **Не перемещать устройства**

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

- **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.



Выбор варианта перемещения устройств в группу администрирования

Шаг 10. Выбор учетных записей для доступа к устройствам

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

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

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

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

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

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

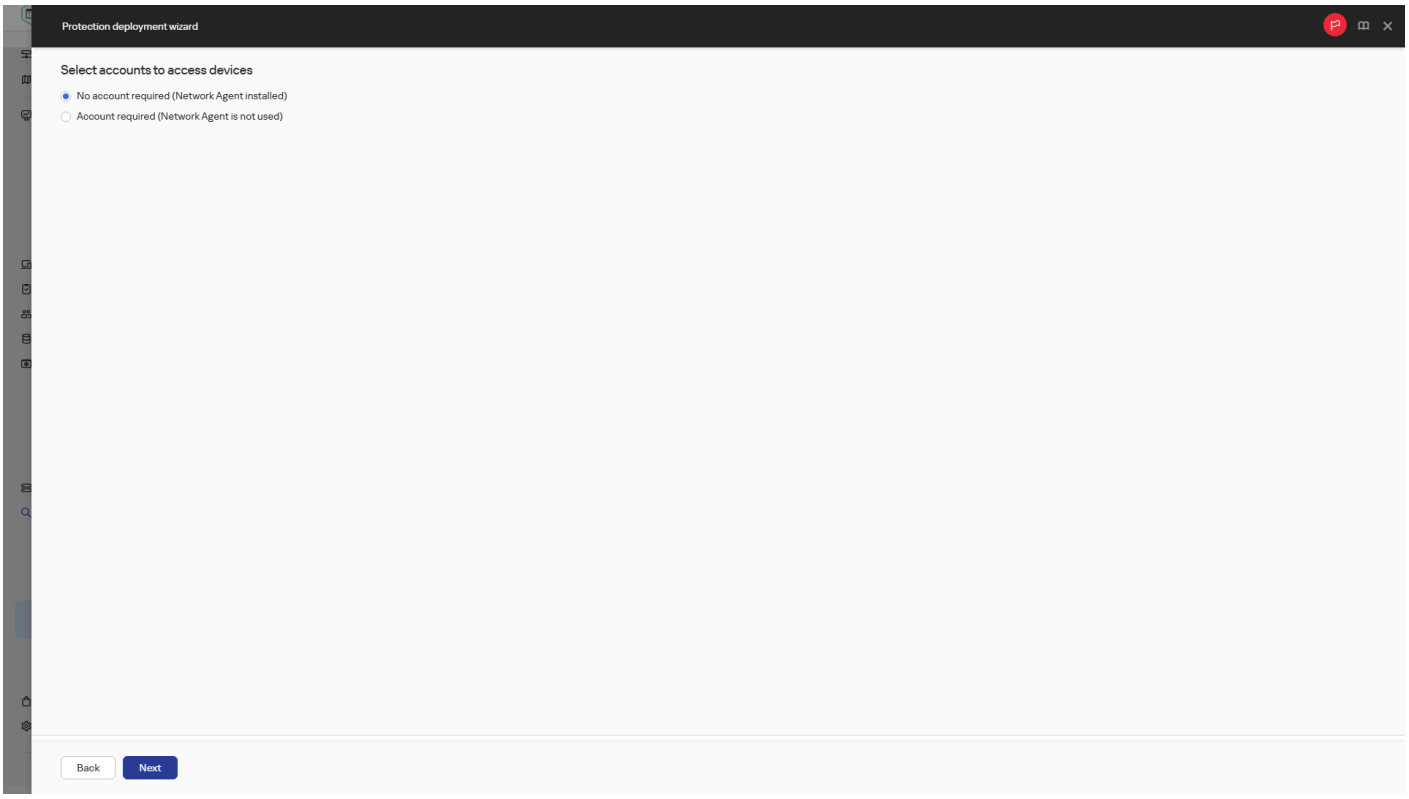
  - **Локальная или доменная учетная запись**. Если выбран этот вариант, укажите учетную запись пользователя, от имени которой будет запускаться установщик приложения. Нажмите на кнопку **Добавить**, выберите **Локальная или доменная учетная запись** и укажите данные учетной записи пользователя.

    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 приложение 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 Linux поддерживает формат закрытых ключей PEM, а утилита ssh-keygen по умолчанию генерирует SSH-ключи в формате OPENSSH. Формат OPENSSH не поддерживается Kaspersky Security Center Linux. 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>"
  ```



Выбор учетных записей для доступа к устройствам

Шаг 11. Запуск установки

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

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

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

Обновление предыдущей версии Kaspersky Security Center Linux

Вы можете установить Сервер администрирования версии 17 на устройство, на котором установлена предыдущая версия Сервера администрирования (начиная с версии 13). При обновлении до версии 17 все данные и параметры предыдущей версии Сервера администрирования сохраняются.

Предварительные требования

- Перед началом обновления необходимо создать резервную копию данных Сервера администрирования.
- При обновлении Сервера администрирования версии 16 или более ранней до версии 16.1 или выше включена двухфакторная аутентификация. Дополнительные сведения см. в статье О двухфакторной аутентификации учетной записи.

  Чтобы обеспечить вход пользователей в Web Console с прежними учетными записями с помощью настроенных секретных ключей двухфакторной аутентификации, а скрипты автоматизации OpenAPI продолжали работать после обновления, необходимо выполнить следующие действия:

  - Включение двухфакторной аутентификации для всех пользователей
  - Администраторы должны настроить двухфакторную аутентификацию для собственных учетных записей
  - Исключение учетных записей из двухфакторной аутентификации

    Если требуется, добавьте учетные записи интеграций, используемые для запуска скриптов через OpenAPI, в список исключений.
- Убедитесь, что вы используете те версии операционной системы и СУБД, которые поддерживаются Сервером администрирования версии 17. При необходимости вы можете перенести Сервер администрирования на другое устройство с более поздними версиями операционной системы и СУБД.
- При обновлении Сервера администрирования с версии 15.4 или более ранней до версии 16 или выше создайте базу данных для IAM на сервере СУБД. Имя этой базы данных должно отличаться от имени базы данных, установленной для работы с Kaspersky Security Center Linux.

  - Для PostgreSQL выполните команду:

    ```
    sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
    ```
  - Для MariaDB выполните команду:

    ```
    sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
    ```

- При обновлении Сервера администрирования с версии 15.4 или более ранней до версии 16 или более поздней подготовьте файл ответов с новыми параметрами для IAM. Список обязательных параметров приведен в статье Установка Kaspersky Security Center Linux в тихом режиме. Добавьте переменную среды `KLAUTOANSWERS`. В качестве значения переменной укажите путь к файлу с ответами.

- Сделайте доступным порт, который используется процессом kliam для аутентификации протокола OpenID Connect. Значение по умолчанию – 4444. Описание параметра `trusted` см. в статье Параметры установки Kaspersky Security Center Web Console.

Этапы

1 Обновление Сервера администрирования

Вы можете обновить версию Сервера администрирования одним из следующих способов:

- С помощью установочного файла Kaspersky Security Center Linux.
- 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 каким-либо другим приложением.

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

2 Запуск скрипта postinstall.pl (необязательный шаг)

Если файл ответов не содержит параметров IAM или файл ответов не найден, во время обновления в терминале отображается сообщение о необходимости запустить скрипт postinstall.pl.

На этом этапе сценария выполните следующее:

1. В операционной системе Сервера администрирования создайте непривилегированную учетную запись пользователя ksciam, которая должна быть членом группы kladmins:

   ```
   adduser ksciam
   gpasswd -a ksciam kladmins
   usermod -g kladmins ksciam
   ```

2. Запустите скрипт /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl под учетной записью с привилегиями root для настройки Сервера администрирования после обновления. При отображении запроса введите следующие параметры:

   1. Введите FQDN сервера IAM. Вам нужно использовать DNS-имя Сервера администрирования, которое было указано при установке Kaspersky Security Center Linux.

   2. Введите имя учетной записи для запуска службы IAM. Учетная запись должна быть членом указанной группы безопасности. По умолчанию используется учетная запись ksciam.

3. Выберите СУБД, которую вы установили для работы со службой IAM:

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

4. Введите адрес СУБД IAM, который будет использоваться службой IAM.
5. Введите номер порта СУБД IAM. Этот порт используется для связи со службой IAM. По умолчанию используются следующие порты:

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

6. Введите имя базы данных IAM, которое будет использоваться службой IAM. Имя базы данных, используемой службой IAM, должно отличаться от имени базы данных, используемой Сервером администрирования.

3. Обновление Kaspersky Security Center Web Console
4. **(Не обязательно) Обновление Агента администрирования на устройствах до новой версии.**
5. **Проверка списка разрешений для настройки двухфакторной аутентификации, чтобы убедиться, что он содержит только те учетные записи, которые должны иметь доступ к Серверу администрирования.**

   Просмотрите список разрешений для настройки двухфакторной аутентификации и удалите из него все лишние учетные записи.

Обратите внимание, если вы обновите Сервер администрирования до версии 17, вы не сможете создавать новые инсталляционные пакеты Агента администрирования версии 15 или ниже. Ранее созданные инсталляционные пакеты будут доступны.

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

Обновление Kaspersky Security Center Linux версии 16 или выше

В этом разделе описаны следующие варианты обновления Kaspersky Security Center Linux с версии 16 и выше до последней:

- обновление с помощью инсталляционного файла;
- обновление с помощью резервной копии;
- обновление на узлах отказоустойчивого кластера Kaspersky Security Center Linux.

Обновление Kaspersky Security Center Linux версии 16 или выше с помощью установочного файла

Для обновления Сервера администрирования с версии 16 до последней версии вы можете установить новую версию поверх предыдущей с помощью установочного файла Kaspersky Security Center Linux.

Чтобы обновить Kaspersky Security Center Linux с версии 16 или выше до последней версии с помощью установочного файла:

1. Загрузите установочный файл Kaspersky Security Center Linux с полным пакетом для версии 17 с сайта "Лаборатории Касперского":
   - Для устройств с операционной системой на базе RPM: `ksc64-<version number>.x86_64.rpm`
   - Для устройств с операционной системой на базе Debian: `ksc64_<version number>_amd64.deb`
2. Запустите обновление предыдущей версии Kaspersky Security Center Linux. Выполните одну из следующих команд в терминале командной строки:
   - Для устройств с операционной системой на базе RPM:

     ```
     sudo yum install ./ksc64-<version number>.x86_64.rpm
     ```

   - Для устройств с операционной системой на базе Debian:

     ```
     sudo apt-get install ./ksc64_<version number>_amd64.deb
     ```

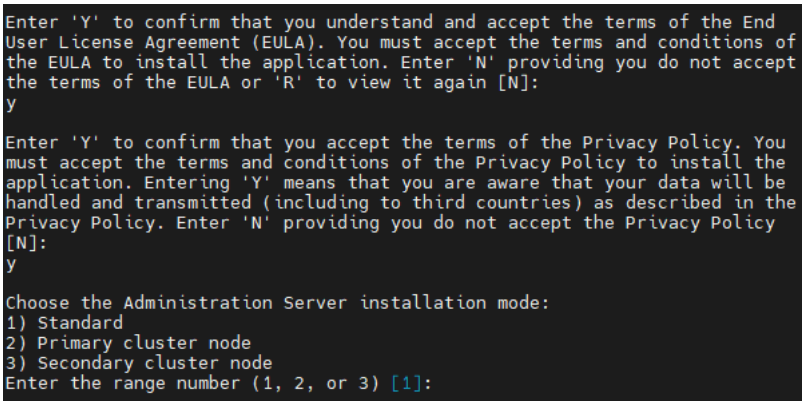
   После успешного выполнения команды создается скрипт `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`. Сообщение об этом отображается в терминале.
3. Запустите скрипт `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` для настройки обновленного Сервера администрирования.

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

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`, чтобы подтвердить, что вы полностью прочитали, поняли и принимаете Политику конфиденциальности, описывающую обработку данных.

   Установка приложения будет продолжена после того, как вы дважды введете `Y`.
5. Введите `1`, чтобы выбрать стандартный режим установки Сервера администрирования.

На картинке ниже показаны последние два шага.



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. Обновите Kaspersky Security Center Web Console до новой версии.

7. 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.

   Выполните следующие команды для активов с операционной системой Linux, чтобы удалить зависимости, которые больше не нужны:

   - Для активов с операционной системой на базе Debian выполните одну из следующих команд:

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - Для активов с операционной системой на базе RPM выполните одну из следующих команд:

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

Обновление Kaspersky Security Center Linux версии 16 или выше с помощью резервной копии

Для обновления Сервера администрирования версии 16 до последней версии 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 Kaspersky Security Center Linux с версии 16 или выше до последней версии с помощью резервной копии:

1. Перед обновлением, выполните резервное копирование данных Сервера администрирования старой версии приложения.

2. Удалите старую версию Kaspersky Security Center Linux.

3. Установите Kaspersky Security Center Linux версии 17 на устройство, на которое ранее был установлен Сервер администрирования.

   Если схема базы данных в резервной копии отличается от схемы, используемой в настоящий момент Сервером администрирования или IAM, данные будут восстановлены в текущую схему.

   Если в резервной копии используется общедоступная схема, должны быть выполнены следующие условия:

   - В базе данных существует общедоступная схема.
   - Вы можете изменить общедоступную схему базы данных под учетной записью СУБД, используемой Сервером администрирования или IAM для доступа к базе данных.

   Иначе восстановление данных завершится с ошибкой.

4. Восстановите данные Сервера администрирования из резервной копии данных, созданной перед обновлением.

5. Установите Kaspersky Security Center Web Console.

   Если приложение Kaspersky Security Center Web Console было установлено ранее, переустановите его с тем же файлом ответов.

   Выполните вход в Kaspersky Security Center Web Console под внутренней учетной записью администратора.

   Процесс инициализации данных обычно занимает до 15 минут после восстановления данных Сервера администрирования, но время зависит от производительности оборудования и размера данных Сервера администрирования. В течение этого периода Kaspersky Security Center Web Console может не подключаться и отображать ошибки.

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.

Выполните следующие команды для активов с операционной системой Linux, чтобы удалить зависимости, которые больше не нужны:

- Для активов с операционной системой на базе Debian выполните одну из следующих команд:

```
sudo apt-get -y autoremove
```

```
sudo apt -y autoremove
```

- Для активов с операционной системой на базе RPM выполните одну из следующих команд:

```
sudo dnf autoremove
```

```
sudo yum autoremove
```

Обновление Kaspersky Security Center Linux версии 16 или выше на узлах отказоустойчивого кластера Kaspersky Security Center Linux

Вы можете установить последнюю версию Сервера администрирования на каждом узле отказоустойчивого кластера Kaspersky Security Center Linux, на котором установлен Сервер администрирования версии 16 или выше. При обновлении до последней версии все данные и параметры предыдущей версии Сервера администрирования сохраняются.

Если вы ранее установили Kaspersky Security Center Linux на устройства локально, также можно обновить Kaspersky Security Center Linux на этих устройствах с помощью установочного файла или с помощью резервной копии.

Не поддерживается обновление Kaspersky Security Center Linux до версии 17 на узлах отказоустойчивого кластера Kaspersky Security Center Linux с помощью установочного файла. Для обновления с предыдущей версии до версии 17 создайте резервную копию данных Сервера администрирования, установите новую версию отказоустойчивого кластера Kaspersky Security Center Linux, а затем восстановите данные Сервера администрирования из резервной копии. Это ограничение актуально и для георасределенного кластера.

Чтобы обновить Kaspersky Security Center Linux версии 16 на узлах отказоустойчивого кластера Kaspersky Security Center Linux:

1. Загрузите установочный файл Kaspersky Security Center Linux с полным пакетом для версии 17 с сайта "Лаборатории Касперского":

   - Для устройств с операционной системой на базе RPM: `ksc64-<version number>-<build number>.x86_64.rpm`
   - Для устройств с операционной системой на базе Debian: `ksc64_<version number>-<build number>_amd64.deb`

2. Остановить кластер.

3. На активном узле кластера выполните следующую команду в терминале командной строки, чтобы запустить обновление:

   - Для устройств с операционной системой на базе RPM:

     ```
     sudo yum install ./ksc64-<version number>-<build number>.x86_64.rpm
     ```

   - Для устройств с операционной системой на базе Debian:

     ```
     sudo apt-get install ./ksc64_<version number>-<build number>_amd64.deb
     ```

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

   При возникновении ошибок ознакомьтесь с решением, описанным в Базе знаний.

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

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

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

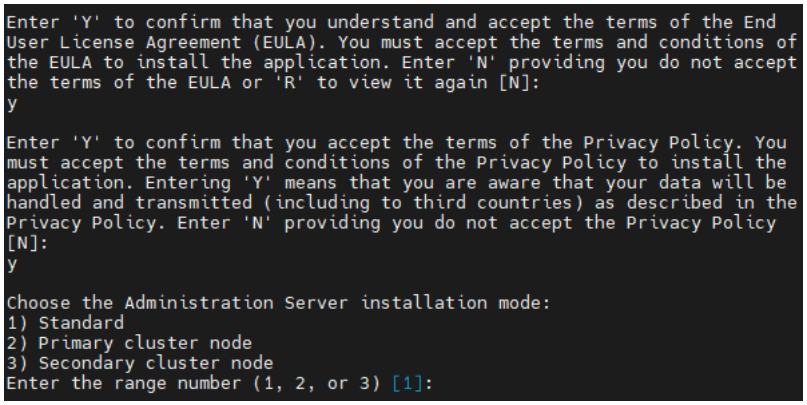
   a. Введите `Y`, чтобы подтвердить, что вы полностью прочитали, поняли и принимаете положения и условия Лицензионного соглашения.

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

   Установка приложения будет продолжена после того, как вы дважды введете `Y`.

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

На картинке ниже показаны последние два шага.



Принятие условий Лицензионного соглашения и Политики конфиденциальности и выбор режима установки 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.

7. Выполните шаги 3–5 на пассивном узле.

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

8. Запустить кластер.

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

9. Для устройств, на которых 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.

   Выполните следующие команды для активов с операционной системой Linux, чтобы удалить зависимости, которые больше не нужны:

   - Для активов с операционной системой на базе Debian выполните одну из следующих команд:

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - Для активов с операционной системой на базе RPM выполните одну из следующих команд:

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

В результате вы установили Сервер администрирования последней версии на узлы отказоустойчивого кластера Kaspersky Security Center Linux.

Обновление Kaspersky Security Center Linux версии 15.4 или ниже

В этом разделе описаны следующие варианты обновления Kaspersky Security Center Linux с версии 15.4 и ниже до версии 16 или выше:

- обновление с помощью инсталляционного файла;
- обновление с помощью резервной копии;
- обновление на узлах отказоустойчивого кластера Kaspersky Security Center Linux.

Каждый вариант обновления Kaspersky Security Center Linux версии 15.4 или ниже до версии 16 или выше включает шаги по созданию и настройке базы IAM на сервере СУБД, созданию непривилегированного пользователя ksciam для запуска службы IAM и добавлению этой учетной записи в группу безопасности kladmins.

Обновление Kaspersky Security Center Linux версии 15.4 или ниже с помощью установочного файла

Для обновления Сервера администрирования с версий 13–15.4 до версии 16 и выше вы можете установить новую версию поверх предыдущей с помощью установочного файла Kaspersky Security Center Linux.

Прежде чем начать, проверьте требования к пользовательскому сертификату

Если вы используете пользовательский сертификат вместо самоподписанного, перед обновлением Kaspersky Security Center Linux до более поздней версии вам нужно убедиться, что сертификат содержит альтернативное имя субъекта (Subject Alternative Name, SAN). Если нет, важно заменить сертификат перед обновлением Kaspersky Security Center Linux. Иначе вы не сможете войти в Web Console после обновления.

Чтобы убедиться, что сертификат включает SAN:

1. На устройстве, на котором установлен Сервер администрирования, выполните команду:

   - Для устройств с операционной системой Linux:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - Для устройств с операционной системой Windows:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Убедитесь, что альтернативное имя субъекта (SAN) присутствует в выходных данных команды и содержит адрес устройства Сервера администрирования.

3. Если альтернативное имя субъекта отсутствует, используйте утилиту klsetsrvcert для замены пользовательского сертификата на сертификат, который соответствует требованиям.

Чтобы обновить Kaspersky Security Center Linux с версии 15.4 или ниже до последней версии с помощью установочного файла:

1. Загрузите установочный файл Kaspersky Security Center Linux с полным пакетом для версии 17 с сайта "Лаборатории Касперского":

   - Для устройств с операционной системой на базе RPM: `ksc64-<version number>.x86_64.rpm`
   - Для устройств с операционной системой на базе Debian: `ksc64_<version number>_amd64.deb`

2. На сервере СУБД создайте базу данных для IAM. Имя базы данных IAM должно отличаться от имени базы данных, используемой Сервером администрирования.

   - Для PostgreSQL выполните команду:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - Для MariaDB выполните команду:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

3. Создайте непривилегированную учетную запись ksciam, добавьте ее в группу безопасности kladmins, а затем установите группу kladmins в качестве основной группы для учетной записи ksciam. Для этого последовательно выполните следующие команды:

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

4. Запустите обновление предыдущей версии Kaspersky Security Center Linux. Выполните одну из следующих команд в терминале командной строки:

   - Для устройств с операционной системой на базе RPM:

     ```
     sudo yum install ./ksc64-<номер версии>.x86_64.rpm
     ```

   - Для устройств с операционной системой на базе Debian:

     ```
     sudo apt-get install ./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.

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

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

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

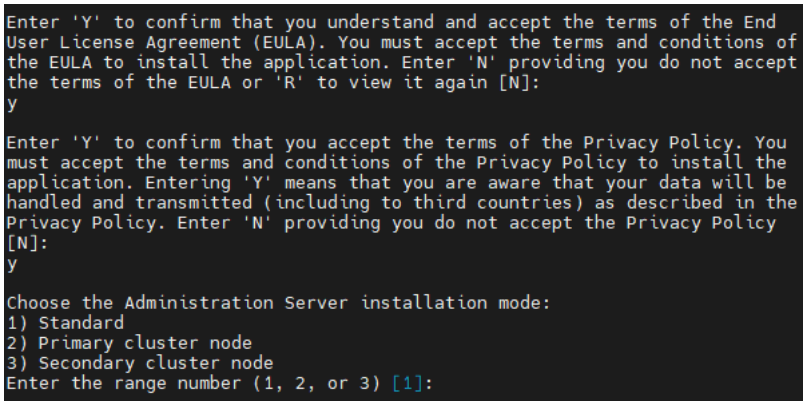
   a. Введите `Y`, чтобы подтвердить, что вы полностью прочитали, поняли и принимаете положения и условия Лицензионного соглашения.

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

   Установка приложения будет продолжена после того, как вы дважды введете `Y`.

7. Введите `1`, чтобы выбрать стандартный режим установки Сервера администрирования.

   На картинке ниже показаны последние два шага.



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

8. Далее скрипт настраивает и завершает обновление Сервера администрирования. Во время обновления вы не можете изменить параметры Сервера администрирования, которые были изменены до обновления. При отображении запроса введите следующие параметры:

   a. Введите FQDN сервера IAM.

      Вам нужно использовать DNS-имя Сервера администрирования, которое было указано при установке Kaspersky Security Center Linux.

   b. Введите имя учетной записи для запуска службы IAM. Учетная запись должна быть членом указанной группы безопасности. По умолчанию используется учетная запись ksciam.

   c. Выберите СУБД, которую вы установили для работы со службой IAM:

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

   d. Введите адрес СУБД IAM, который будет использоваться службой IAM.

e. Введите номер порта СУБД IAM. Этот порт используется для связи со службой IAM. По умолчанию используются следующие порты:

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

f. Введите имя базы данных IAM, которое будет использоваться службой IAM. Имя базы данных, используемой службой IAM, должно отличаться от имени базы данных, используемой Сервером администрирования.

g. Введите учетную запись и пароль СУБД, которая будет использоваться службой IAM.

h. Если вы установили PostgreSQL или Postgres Pro, вы можете указать схему базы данных, которая будет использоваться IAM. Для этого укажите имя схемы.

Если вы не хотите использовать пользовательскую схему, нажмите `ENTER`. В этом случае будет использоваться общедоступная схема.

> Имя схемы чувствительно к регистру. Используйте только строчные буквы.
> Не указывайте зарезервированные имена схем IAM: `client, iam, ksc, locker, pat, scope, voltron`.

9. Обновите Kaspersky Security Center Web Console до новой версии.

10. 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.

Выполните следующие команды для активов с операционной системой Linux, чтобы удалить зависимости, которые больше не нужны:

- Для активов с операционной системой на базе Debian выполните одну из следующих команд:

```
sudo apt-get -y autoremove
```

```
sudo apt -y autoremove
```

- Для активов с операционной системой на базе RPM выполните одну из следующих команд:

```
sudo dnf autoremove
```

```
sudo yum autoremove
```

Обновление Kaspersky Security Center Linux версии 15.4 или ниже с помощью резервной копии

Чтобы обновить Сервер администрирования версий 14.2-15.4 до версии 16 и выше, вы можете создать резервную копию данных Сервера администрирования и восстановить ее после установки новой версии Kaspersky Security Center Linux. Если при установке возникли проблемы, вы можете восстановить предыдущую версию Сервера администрирования, используя созданную перед обновлением резервную копию данных Сервера.

Предварительные требования

1. **Проверьте требования к пользовательскому сертификату**

   Если вы используете пользовательский сертификат вместо самоподписанного, перед обновлением Kaspersky Security Center Linux до более поздней версии вам нужно убедиться, что сертификат содержит альтернативное имя субъекта (Subject Alternative Name, SAN). Если нет, важно заменить сертификат перед обновлением Kaspersky Security Center Linux. Иначе вы не сможете войти в Web Console после обновления.

   Чтобы убедиться, что сертификат включает SAN:

   1. На устройстве, на котором установлен Сервер администрирования, выполните команду:

      - Для устройств с операционной системой Linux:

        ```
        sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
        ```

      - Для устройств с операционной системой Windows:

        ```
        certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
        ```

   2. Убедитесь, что альтернативное имя субъекта (SAN) присутствует в выходных данных команды и содержит адрес устройства Сервера администрирования.

   3. Если альтернативное имя субъекта отсутствует, используйте утилиту klsetsrvcert для замены пользовательского сертификата на сертификат, который соответствует требованиям.

2. Выполните резервное копирование данных Сервера администрирования старой версии приложения.

Процедура обновления с предыдущей версии

Чтобы обновить Kaspersky Security Center Linux версии 15.4 или ниже до последней версии с помощью резервной копии:

1. Удалите старую версию Kaspersky Security Center Linux.
2. На сервере СУБД создайте базу данных для IAM. Имя базы данных IAM должно отличаться от имени базы данных, используемой Сервером администрирования.
   - Для PostgreSQL выполните команду:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - Для MariaDB выполните команду:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

3. Создайте непривилегированную учетную запись ksciam, добавьте ее в группу безопасности kladmins, а затем установите группу kladmins в качестве основной группы для учетной записи ksciam. Для этого последовательно выполните следующие команды:

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

4. Установите Kaspersky Security Center Linux версии 17 на устройство, на которое ранее был установлен Сервер администрирования.

   Если схема базы данных в резервной копии отличается от схемы, используемой в настоящий момент Сервером администрирования или IAM, данные будут восстановлены в текущую схему.

   Если в резервной копии используется общедоступная схема, должны быть выполнены следующие условия:

   - В базе данных существует общедоступная схема.
   - Вы можете изменить общедоступную схему базы данных под учетной записью СУБД, используемой Сервером администрирования или IAM для доступа к базе данных.

   Иначе восстановление данных завершится с ошибкой.

5. Восстановите данные Сервера администрирования из резервной копии данных, созданной перед обновлением.
6. Настройте проверку сертификата Сервером администрирования и сервером IAM.
7. Установите Kaspersky Security Center Web Console.

   Если приложение Kaspersky Security Center Web Console было установлено ранее, переустановите его с тем же файлом ответов.

   Выполните вход в Kaspersky Security Center Web Console под внутренней учетной записью администратора.

Процесс инициализации данных обычно занимает до 15 минут после восстановления данных Сервера администрирования, но время зависит от производительности оборудования и размера данных Сервера администрирования. В течение этого периода Kaspersky Security Center Web Console может не подключаться и отображать ошибки.

8. 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.

   Выполните следующие команды для активов с операционной системой Linux, чтобы удалить зависимости, которые больше не нужны:

   - Для активов с операционной системой на базе Debian выполните одну из следующих команд:

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - Для активов с операционной системой на базе RPM выполните одну из следующих команд:

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

Обновление Kaspersky Security Center Linux с версии 15.4 или ниже на узлах отказоустойчивого кластера Kaspersky Security Center Linux

Вы можете установить Сервер администрирования версии 16 и выше на каждом узле отказоустойчивого кластера Kaspersky Security Center Linux, на котором установлен Сервер администрирования версии 14–15.4. При обновлении все данные и параметры предыдущей версии Сервера администрирования сохраняются.

Прежде чем начать, проверьте требования к пользовательскому сертификату

Если вы используете пользовательский сертификат вместо самоподписанного, перед обновлением Kaspersky Security Center Linux до более поздней версии вам нужно убедиться, что сертификат содержит альтернативное имя субъекта (Subject Alternative Name, SAN). Если нет, важно заменить сертификат перед обновлением Kaspersky Security Center Linux. Иначе вы не сможете войти в Web Console после обновления.

Чтобы убедиться, что сертификат включает SAN:

1. На устройстве, на котором установлен Сервер администрирования, выполните команду:

   - Для устройств с операционной системой Linux:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   - Для устройств с операционной системой Windows:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Убедитесь, что альтернативное имя субъекта (SAN) присутствует в выходных данных команды и содержит адрес устройства Сервера администрирования.

3. Если альтернативное имя субъекта отсутствует, используйте утилиту klsetsrvcert для замены пользовательского сертификата на сертификат, который соответствует требованиям.

Если вы ранее установили Kaspersky Security Center Linux на устройства локально, также можно обновить Kaspersky Security Center Linux на этих устройствах с помощью установочного файла или с помощью резервной копии.

Чтобы обновить Kaspersky Security Center Linux версии 15.4 или ниже на узлах отказоустойчивого кластера Kaspersky Security Center Linux:

1. Загрузите установочный файл Kaspersky Security Center Linux с полным пакетом для версии 17 с сайта "Лаборатории Касперского":

   - Для устройств с операционной системой на базе RPM: `ksc64-<version number>-<build number>.x86_64.rpm`

   - Для устройств с операционной системой на базе Debian: `ksc64_<version number>-<build number>_amd64.deb`

2. Остановить кластер.

3. На сервере СУБД создайте базу данных для IAM. Имя базы данных IAM должно отличаться от имени базы данных, используемой Сервером администрирования.

   - Для PostgreSQL выполните команду:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - Для MariaDB выполните команду:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

4. Создайте непривилегированную учетную запись ksciam, добавьте ее в группу безопасности kladmins, а затем установите группу kladmins в качестве основной группы для учетной записи ksciam. Для этого последовательно выполните следующие команды:

```
sudo adduser ksciam
sudo gpasswd -a ksciam kladmins
sudo usermod -g kladmins ksciam
```

5. На активном узле кластера выполните одну из следующих команд в терминале командной строки, чтобы запустить обновление:

   - Для устройств с операционной системой на базе RPM:

     ```
     sudo yum install ./ksc64-<номер версии>-<номер сборки>.x86_64.rpm
     ```

   - Для устройств с операционной системой на базе Debian:

     ```
     sudo apt-get install ./ksc64_<номер версии>-<номер сборки>_amd64.deb
     ```

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

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

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

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

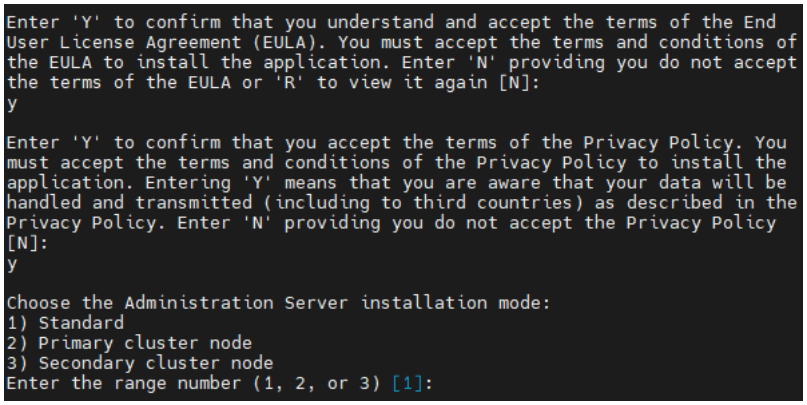
   a. Введите `Y`, чтобы подтвердить, что вы полностью прочитали, поняли и принимаете положения и условия Лицензионного соглашения.

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

   Установка приложения будет продолжена после того, как вы дважды введете `Y`.

8. Выберите узел, на котором вы выполняете обновление, указав `2`.

На картинке ниже показаны последние два шага.



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

9. Далее скрипт настраивает и завершает обновление Сервера администрирования. Во время обновления вы не можете изменить параметры Сервера администрирования, которые были изменены до обновления. При отображении запроса введите следующие параметры:

   a. Введите FQDN сервера IAM.

      Вам нужно использовать DNS-имя Сервера администрирования, которое было указано при установке Kaspersky Security Center Linux.

   b. Введите имя учетной записи для запуска службы IAM. Учетная запись должна быть членом указанной группы безопасности. По умолчанию используется учетная запись ksciam.

   c. Выберите СУБД, которую вы установили для работы со службой IAM:

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

   d. Введите адрес СУБД IAM, который будет использоваться службой IAM.

   e. Введите номер порта СУБД IAM. Этот порт используется для связи со службой IAM. По умолчанию используются следующие порты:

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

   f. Введите имя базы данных IAM, которое будет использоваться службой IAM. Имя базы данных, используемой службой IAM, должно отличаться от имени базы данных, используемой Сервером администрирования.

   g. Введите учетную запись и пароль СУБД, которая будет использоваться службой IAM.

10. Выполните шаг 5 на пассивном узле.

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

11. Запустить кластер.

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

12. Для устройств, на которых 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.

    Выполните следующие команды для активов с операционной системой Linux, чтобы удалить зависимости, которые больше не нужны:

    - Для активов с операционной системой на базе Debian выполните одну из следующих команд:

      ```
      sudo apt-get -y autoremove
      ```

      ```
      sudo apt -y autoremove
      ```

    - Для активов с операционной системой на базе RPM выполните одну из следующих команд:

      ```
      sudo dnf autoremove
      ```

      ```
      sudo yum autoremove
      ```

    В результате вы установили Сервер администрирования последней версии на узлы отказоустойчивого кластера Kaspersky Security Center Linux.

Обновление Kaspersky Security Center Web Console

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

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

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

- Для операционных систем на базе Debian: ksc-web-console-<номер_сборки>.x86_64.deb.
- Для операционных систем на базе RPM: ksc-web-console-<номер_сборки>.x86_64.rpm.

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

Чтобы обновить Kaspersky Security Center Web Console:

1. Убедитесь, что на устройстве, на котором вы хотите обновить Kaspersky Security Center Web Console, работает один из поддерживаемых дистрибутивов Linux.

2. Прочитайте и примите Лицензионное соглашение. Если в состав дистрибутива Kaspersky Security Center Linux не входит TXT файл с текстом Лицензионного соглашения, вы можете загрузить этот файл с сайта "Лаборатории Касперского". Если вы не принимаете условия Лицензионного соглашения, не обновляйте Kaspersky Security Center Web Console с помощью установочного файла.

3. Используйте тот же файл ответов, который вы подготовили перед установкой Kaspersky Security Center Web Console. Имя файла ответов ksc-web-console-setup.json. Файл расположен в директории /etc/ksc-web-console-setup.json.

   Если при установке Kaspersky Security Center Web Console вы указали значения параметров `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount`, и `natsMessageQueueAccount`, убедитесь, что все эти параметры указаны в файле ответов.

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

   Пример файла ответов с минимальным набором параметров

   Набор параметров файла ответов зависит от версии Сервера администрирования, к которому подключено приложение Kaspersky Security Center Web Console:

   - Сервер администрирования версии 16 и выше

     Пример файла ответов с минимальным набором параметров для входа на Сервер администрирования версии 16 и выше:

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
             "Administration Server v16": {
                 "iamHost": "ksc16.example.com",
                 "iamOAuthPort": 4444,
                 "iamProxyPort": 9050,
                 "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
                 "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
                 "kscPort": 13299,
                 "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
             }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

   - Сервер администрирования версии 15.4 и выше

     Пример файла ответов с минимальным набором параметров для входа на Сервер администрирования версии 15.4 и ниже:

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
              "Administration Server v15.4": {
                  "kscHost": "ksc.example.com",
                  "kscPort": 13299,
                  "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
              }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

Вы можете установить Kaspersky Security Center Web Console на том же устройстве, что и Сервер администрирования, или на другом устройстве. Если приложение Kaspersky Security Center Web Console установлено на другом устройстве, адрес Kaspersky Security Center Web Console (параметр `address`) и адрес Сервера администрирования (параметр `iamHost` или `kscHost`) отличаются. Если приложение Kaspersky Security Center Web Console установлено на одном устройстве с Сервером администрирования, эти параметры имеют одинаковые значения.

Значение `iamHost` должно совпадать с адресом IAM, который вы указали при установке Сервера администрирования. Для получения указанного адреса IAM выполните следующую команду на устройстве с установленным Сервером администрирования:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Подробную информацию см. в статье Параметры установки Kaspersky Security Center Web Console.

Вы можете добавить несколько Серверов администрирования разных версий в список доверенных серверов. В этом случае Серверы могут использовать разные способы аутентификации.

Если вы хотите обновить приложение Kaspersky Security Center Web Console, подключенное к Серверу администрирования, который установлен на узлах отказоустойчивого кластера Kaspersky Security Center Linux, в файле ответа укажите параметр установки trusted, чтобы разрешить отказоустойчивому кластеру Kaspersky Security Center Linux подключаться к Kaspersky Security Center Web Console.

Компоненты **параметра установки** `trusted`

Если вы подключаетесь к отказоустойчивому кластеру Kaspersky Security Center Linux с использованием доменной аутентификации с SSO, укажите параметры установки trusted: при подключении Kaspersky Security Center Web Console к Серверу администрирования версии 16 и выше будет использоваться доменная аутентификация с единым входом (SSO), предоставляемая Identity and Access Manager (IAM). В этом случае укажите параметры установки `trusted` следующим образом:

```
"trusted":  {
        "<Имя Сервера администрирования>": {
                "iamHost": "ksc-iam.example.com",
                "iamOAuthPort": 4444,
                "iamProxyPort": 9050,
                "iamCertPath": "<папка общих данных>/iam/main_certificate.pem",
                "iamPATPath": "<папка общих данных>/iam/initial_token.txt",
                "kscPort": 13299,
                "kscCertPath": "<папка общих данных>/1093/cert/klserver.cer"
        }
}
```

где:

- `<Имя Сервера администрирования>` – имя отказоустойчивого кластера Kaspersky Security Center Linux, которое будет отображаться в окне входа в Kaspersky Security Center Web Console.
- `iamHost` – адрес устройства, на котором установлены Сервер администрирования и IAM. Если вы создали дополнительный сетевой адаптер при подготовке узлов кластера, используйте FQDN или имя устройства адаптера в качестве адреса отказоустойчивого кластера Kaspersky Security Center Linux. В ином случае укажите FQDN или имя устройства стороннего балансировщика нагрузки, который вы используете.

  Значение `iamHost` должно совпадать с адресом IAM, указанным при установке Сервера администрирования. Для получения указанного адреса IAM выполните следующую команду на устройстве с установленным Сервером администрирования:

  `grep "iam_address:" <папка общих данных>/iam/iam_config.yaml`

- `iamOAuthPort` – порт, который используется для обмена токенами аутентификации по протоколу аутентификации OpenID Connect (значение по умолчанию – 4444). Этот порт используется как для связи между Сервером Kaspersky Security Center Web Console и Сервером администрирования, так и между браузером (используется с Kaspersky Security Center Web Console) и Сервером администрирования.

- `iamProxyPort` – порт, который используется для подключения Сервера Kaspersky Security Center Web Console к Серверу администрирования (значение по умолчанию – 9050).

- `iamCertPath` – это путь к IAM-сертификату. IAM-сертификат создается автоматически при первом запуске Сервера администрирования. Сертификат хранится на устройстве, на котором установлен Сервер администрирования. Путь по умолчанию к сертификату: `< общая папка данных >/iam/main_certificate.pem`. Сертификат находится в общем хранилище данных отказоустойчивого кластера Kaspersky Security Center Linux. Самоподписанный IAM-сертификат обновляется автоматически.

- `iamPATPath` – путь к токену, который используется для регистрации Kaspersky Security Center Web Console в качестве OAuth-клиента в IAM. Этот файл создается автоматически при первом запуске Сервера администрирования. Токен хранится на устройстве, на котором установлен Сервер администрирования. Путь по умолчанию к токену: <общая папка данных>/iam/initial_token.txt. Токен находится в общем хранилище данных отказоустойчивого кластера Kaspersky Security Center Linux. Токен действует бессрочно и не требует ротации.

- `kscPort` – порт OpenAPI, который Kaspersky Security Center Web Console, использует для подключения к Серверу администрирования (по умолчанию 13299).

- `kscCertPath` – сертификат Сервера администрирования, находящийся в общем хранилище данных отказоустойчивого кластера Kaspersky Security Center Linux. Путь по умолчанию к файлу сертификата: `< общая папка данных >\1093\cert\klserver.cer`.

  > Скопируйте файл сертификата Сервера администрирования (по пути, указанному в параметре `kscCertPath`), файл IAM-сертификата (по пути, указанному в параметре `iamCertPath`) и файл токена (по пути, указанному в параметре `iamPATPath`) из общего хранилища данных на устройство, на котором вы устанавливаете Kaspersky Security Center Web Console. Укажите локальный путь к сертификату Сервера администрирования.

Если вы подключаете Kaspersky Security Center Web Console к Серверу администрирования версии 15.4 и ниже, аутентификация будет выполняться с использованием имени и пароля доменного пользователя или внутреннего пользователя. В этом случае укажите параметры установки trusted следующим образом:

```
"trusted":  {
        "<Имя Сервера администрирования>": {
                "kscHost": "ksc.example.com",
                "kscPort": 13299,
                "kscCertPath": "<папка общих данных>/1093/cert/klserver.cer"
        }
}
```

где:

- `< Имя Сервера администрирования >` – имя отказоустойчивого кластера Kaspersky Security Center Linux, которое будет отображаться в окне входа в Kaspersky Security Center Web Console.

- `kscHost` – это адрес Сервера администрирования (FQDN или имя устройства). Если вы создали дополнительный сетевой адаптер при подготовке узлов кластера, используйте адрес адаптера в качестве адреса отказоустойчивого кластера Kaspersky Security Center Linux. В противном случае укажите адрес стороннего балансировщика нагрузки, который вы используете.

- `kscPort` – порт OpenAPI, который Kaspersky Security Center Web Console, использует для подключения к Серверу администрирования (по умолчанию 13299).

- `kscCertPath` – сертификат Сервера администрирования, находящийся в общем хранилище данных отказоустойчивого кластера Kaspersky Security Center Linux. Путь по умолчанию к файлу сертификата: `<общая папка данных>\1093\cert\klserver.cer`. Скопируйте файл сертификата из общего хранилища данных на устройство, на котором вы устанавливаете Kaspersky Security Center Web Console. Укажите локальный путь к сертификату Сервера администрирования.

Приложение Kaspersky Security Center Web Console невозможно обновить с помощью того же установочного файла. Если вы хотите изменить параметры файла ответов и использовать этот файл для переустановки приложения, вам нужно сначала удалить приложение, а затем установить его снова с новым файлом ответов.

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

   Чтобы обновить предыдущую версию Kaspersky Security Center Web Console, выполните одну из следующих команд:

   - Для устройств с операционной системой на базе RPM:
     ```
     sudo yum install ksc-web-console-<build_number>.x86_64.rpm
     ```

   - Для устройств с операционной системой на базе Debian:
     ```
     sudo apt-get install ksc-web-console-<build_number>.x86_64.deb
     ```

   Начнется распаковка установочного файла. Пожалуйста, дождитесь завершения установки.

5. Перезапустите все службы Kaspersky Security Center Web Console, выполнив следующую команду:
   ```
   sudo systemctl restart KSC*
   ```

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

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

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

Чтобы обновить Kaspersky Security Center Web Console:

1. Убедитесь, что на устройстве, на котором вы хотите обновить Kaspersky Security Center Web Console, работает один из поддерживаемых дистрибутивов Linux.

2. Прочитайте и примите Лицензионное соглашение. Если в состав дистрибутива Kaspersky Security Center Linux не входит TXT файл с текстом Лицензионного соглашения, вы можете загрузить этот файл с сайта "Лаборатории Касперского". Если вы не принимаете условия Лицензионного соглашения, не обновляйте Kaspersky Security Center Web Console с помощью установочного файла.

3. Используйте тот же файл ответов, который вы подготовили перед установкой Kaspersky Security Center Web Console. Имя файла ответов ksc-web-console-setup.json. Файл расположен в директории /etc/ksc-web-console-setup.json.

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

   Пример файла ответов с минимальным набором параметров

   Набор параметров файла ответов зависит от версии Сервера администрирования, к которому подключено приложение Kaspersky Security Center Web Console:

   - Сервер администрирования версии 16 и выше

     Пример файла ответов с минимальным набором параметров для входа на Сервер администрирования версии 16 и выше:

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
             "Administration Server v16": {
                 "iamHost": "ksc16.example.com",
                 "iamOAuthPort": 4444,
                 "iamProxyPort": 9050,
                 "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
                 "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
                 "kscPort": 13299,
                 "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
             }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

   - Сервер администрирования версии 15.4 и выше

     Пример файла ответов с минимальным набором параметров для входа на Сервер администрирования версии 15.4 и ниже:

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
              "Administration Server v15.4": {
                  "kscHost": "ksc.example.com",
                  "kscPort": 13299,
                  "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
              }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

   Вы можете установить Kaspersky Security Center Web Console на том же устройстве, что и Сервер администрирования, или на другом устройстве. Если приложение Kaspersky Security Center Web Console установлено на другом устройстве, адрес Kaspersky Security Center Web Console (параметр `address`) и адрес Сервера администрирования (параметр `iamHost` или `kscHost`) отличаются. Если приложение Kaspersky Security Center Web Console установлено на одном устройстве с Сервером администрирования, эти параметры имеют одинаковые значения.

   Значение `iamHost` должно совпадать с адресом IAM, который вы указали при установке Сервера администрирования. Для получения указанного адреса IAM выполните следующую команду на устройстве с установленным Сервером администрирования:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Подробную информацию см. в статье Параметры установки Kaspersky Security Center Web Console.

Вы можете добавить несколько Серверов администрирования разных версий в список доверенных серверов. В этом случае Серверы могут использовать разные способы аутентификации.

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

   ```
   DIGSIG_ELF_MODE=1
   ```

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

   Если этот пакет не установлен, выполните следующую команду:

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

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

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

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

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

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

8. Обновите оперативную память дисков:

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

   Перезагрузите систему.

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

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

   ```
   sudo apt-get install ksc-web-console-<build_number>.x86_64.deb
   ```

   Начнется распаковка установочного файла. Пожалуйста, дождитесь завершения установки.

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

    ```
    sudo systemctl restart KSC*
    ```

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

Перенос данных в приложение Kaspersky Security Center Linux

Выберите **Сценарий миграции на Kaspersky Security Center с использованием скрипта быстрой установки**, если выполняются все условия:

- не требуется раздельная установка Сервера администрирования и СУБД на отдельные устройства;
- ОС для Сервера администрирования Ubuntu, Astra Linux, CentOS или РЕД ОС;
- подходит PostgreSQL, MySQL или MariaDB для нового Сервера администрирования.

Выберите **Общее руководство по миграции на новый сервер Kaspersky Security Center**, если хотя бы одно из условий выполняется:

- требуется раздельная установка Сервера администрирования и СУБД на разные устройства;
- ОС и СУБД для Сервера администрирования не входят в перечень поддерживаемых скриптом быстрой установки.

Выберите **Перенос данных в Kaspersky Security Center с помощью мастера переноса данных**, если:

- тип СУБД прежнего Сервера администрирования и нового Kaspersky Security Center не совпадают и не используется Microsoft SQL Server;
- у вас есть опыт работы с переключением управляемых устройств на новый Сервер администрирования с помощью задач и утилит Kaspersky Security Center.

Дополнительные сведения об особенностях и ограничениях смотрите на страницах руководств.

Сценарий миграции на Kaspersky Security Center Linux с использованием скрипта быстрой установки

Сценарий включает примеры миграции решения с переносом данных на новое устройство с установленным Сервером администрирования для:

- Миграции с Kaspersky Security Center Windows (СУБД MS SQL и PostgreSQL) на Kaspersky Security Center Linux (СУБД PostgreSQL).
- Переноса Kaspersky Security Center Linux (СУБД PostgreSQL) для замены оборудования.

Развертывание нового Сервера администрирования выполняется с использованием скрипта быстрой установки.

Доступные способы переноса данных в MySQL и MariaDB изложены в этом сценарии. При наличии органичений сценария используйте другие способы, описанные в разделе по миграции на Kaspersky Security Center Linux.

1 Предварительные действия перед созданием резервной копии

Этот шаг содержит инструкции по подготовке ранее настроенного Сервера администрирования для дальнейшей миграции на новый Сервер администрирования Kaspersky Security Center Linux. Подготовка состоит из следующих этапов:

1. Проверка версии Сервера администрирования для создания совместимой с Kaspersky Security Center Linux резервной копии.

   Все актуальные версии **Kaspersky Security Center Linux** поддерживают перенос данных с обновлением на более новую версию приложения. Создание и восстановление резервных копий возможно только в рамках одного типа СУБД.

   Для **Kaspersky Security Center Windows** необходимо проверить версию Сервера администрирования в **Свойства** → **Общие** → **Версия**. Если версия ниже, чем 15.1.0.28509, обновите Kaspersky Security Center Windows до последней версии.

   Обновление Kaspersky Security Center Windows до последней версии

   1. На сайте "Лаборатории Касперского" скачайте дистрибутив, соответствующий языку локализации установленного Сервера администрирования: `Version 15.1.0.28509 | Windows | Full distributive`.

      Исполняемый файл сохраняется в папку **Загрузки** со следующим названием: `ksc_15.1_<build number>_full_<language>.exe`.

   2. Скопируйте дистрибутив на Сервер администрирования.

   3. Запустите от администратора исполняемый файл `ksc_15.1_<build number>_full_<language>.exe`.

   4. В открывшемся окне нажмите на ссылку **Установить Kaspersky Security Center**.

      Запустится мастер установки Сервера администрирования.

   5. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения следующих документов** установите флажки:

      - **Условия и положения настоящего Лицензионного соглашения**.
      - **Политику конфиденциальности, которая описывает обработку данных**.

   6. Выберите **Обновить Сервер администрирования и консоль на основе веб-интерфейса (рекомендуется)** и перейдите к следующему шагу.

   7. Создайте новую резервную копию, выберите опцию **Я хочу создать резервную копию данных** и пройдите мастер создания резервной копии.

   8. Нажмите **Обновить**.

9. Во время обновления в мастере установки Web Console подтвердите все шаги мастера для обновления версии.

   Процесс установки обновления Сервера администрирования займет некоторые время. После завершения мастера установки Консоль администрирования может не принимать подключения до завершения инициализации базы данных.

10. Дождитесь полного завершения процедуры обновления.

2. Проверка выполнения требований к сертификату Сервера администрирования.

   Перед созданием резервной копии вам нужно убедиться, что сертификат содержит альтернативное имя субъекта (Subject Alternative Name, SAN). Если нет, важно заменить сертификат, иначе вы не сможете войти в Web Console после восстановления из резервной копии.

   Чтобы проверить, что сертификат включает альтернативное имя субъекта:

   - Для устройств с операционной системой Windows:

     a. В Консоли администрирования выберите Сервер администрирования, для которого требуется проверка.

     b. В контекстном меню выберите пункт **Свойства** → **Общие** → **Просмотреть сертификат Сервера**.

     c. В открывшемся окне проверьте значение пункта **Альтернативное имя субъекта**.

   - Для устройств с операционной системой Linux выполните команду:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   Убедитесь, что альтернативное имя субъекта содержит доменное имя (DNS) устройства Сервера администрирования.

   Если значение содержит только внешний IP-адрес без доменного имени (DNS) или значение полностью отсутствует, вручную замените сертификат на соответствующий требованиям работы с Kaspersky Security Center Linux. Замените общий сертификат Сервера администрирования с помощью утилиты klsetsrvcert.

   Замена общего сертификата Сервера администрирования с помощью утилиты klsetsrvcert

   1. Создайте новый сертификат с отложенной датой начала использования на устройствах, выполнив команду:

      - Для Kaspersky Security Center Windows:

        ```
        "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -t CR -g "
        <oldksc.example.internal>" -o "RsaKeyLen:2048"
        ```

      - Для Kaspersky Security Center Linux:

        ```
        /opt/kaspersky/ksc64/sbin/klsetsrvcert -t CR -g "<oldksc.example.internal>" -o "RsaKeyLen:2048"
        ```

      где `"<oldksc.example.internal>"` – FQDN-адрес подключения к Серверу администрирования.

      > Не используйте IP-адрес для этого значения.

2. Назначьте дату начала использования нового сертификата на всех устройствах, выполнив команду:

   - Для Kaspersky Security Center Windows:

     ```
     "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -f "DD-MM-YYYY hh:mm"
     ```

   - Для Kaspersky Security Center Linux:

     ```
     /opt/kaspersky/ksc64/sbin/klsetsrvcert -f "DD-MM-YYYY hh:mm"
     ```

   где дата `"DD-MM-YYYY hh:mm"` минимум на 30 дней больше текущей. По умолчанию период распространения нового сертификата (`CR`) составляет 90 дней.

   > После наступления назначенного времени может потребоваться переустановить Web Console чтобы восстановить к ней доступ и актуализировать сертификат в ее составе.

3. Если необходимо, после миграции на новый Сервер администрирования запустите утилиту klmover, чтобы восстановить соединение устройств с Сервером администрирования. Запуск утилиты может понадобиться, если устройство было выключено весь период распространения сертификата или не подключалось к Серверу администрирования.

2 Создание резервной копии предыдущей установки Сервера администрирования

Создание резервной копии Kaspersky Security Center Windows

1. Из меню **Пуск** → **Kaspersky Security Center** → **Kaspersky Backup Utility** запустите утилиту `klbackup.exe`, расположенную в папке установки Kaspersky Security Center Linux.

   Запустится мастер установки. На ОС Microsoft Windows в режиме Server Core используйте консольную версию утилиты klbackup.

2. На первом шаге выберите **Выполнить резервное копирование данных Сервера администрирования**.

3. На шаге **Параметры резервного копирования** выполните следующие действия:

   a. Нажмите на кнопку **Обзор** и создайте новую папку для сохранения резервной копии отдельно от директории по умолчанию, например `C:\kscbackups`.

   b. Если вы используете Microsoft SQL Server, выберите опцию **Перенос базы данных** → **Перенести в формат Postgres** или **Перенос данных в формате MySQL/MariaDB**.

   Если используется не Microsoft SQL Server, в резервной копии сохранится прежний тип базы данных.

   c. Задайте пароль к резервной копии для защиты от несанкционированного доступа к данным.

4. Дождитесь создания резервной копии и завершите работу утилиты.

В директории создана новая директория с отметкой времени создания резервной копии.

Создание резервной копии Kaspersky Security Center Linux

1. На устройстве с Сервером администрирования в командной строке введите следующую команду:

```
sudo /opt/kaspersky/ksc64/sbin/klbackup -path /root/kscbackups -use_ts
```

2. Дождитесь завершения создания резервной копии.

В директории, указанной после параметра `-path`, будет создана новая директория с отметкой времени создания резервной копии.

После создания резервной копии предыдущего Сервера администрирования, выведите из эксплуатации устройство с Сервером администрирования.

Вывод устройства с Сервером администрирования из эксплуатации

1. Скопируйте полученную резервную копию для переноса данных на устройство администратора.
2. Завершите работу операционной системы Сервера администрирования.
3. Отключите сетевой адаптер от корпоративной сети.
4. Освободите IP-адрес устройства, если планируете использовать его для новой установки Kaspersky Security Center Linux.
5. Убедитесь, что устройство полностью отключено.

Нахождение в сети прежнего Сервера администрирования может вызывать сбои управления устройствами и нарушение входа в Web Console нового Сервера администрирования, а также запуск задачи установки Агента администрирования с подключением к старому серверу.

3 Первоначальная установка Kaspersky Security Center Linux с помощью скрипта быстрой установки

Эта инструкция описывает первоначальное развертывание экземпляра Kaspersky Security Center Linux с использованием скрипта быстрой установки.

Особенности:

- Установка всех компонентов Kaspersky Security Center выполняется на одном устройстве с Сервером администрирования.
- Скрипт быстрой установки автоматизирует только настройку и установку приложения Kaspersky Security Center. Администратор самостоятельно настраивает имя устройства с Сервером администрирования в операционной системе, работу сетевых адаптеров, сетевые экраны безопасности на уровне операционной системы и настраивает оборудование.
- Для Сервера администрирования используется операционная система и СУБД из таблицы:

Версия операционной системы.	СУБД
Ubuntu Server 26.04 LTS	PostgreSQL 18 MySQL 8.4 (сборка 8.4.10)
РЕД ОС 8	PostgreSQL 16 MariaDB 10.11 (сборка 10.11.18)
Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8.5)	PostgreSQL 15 MariaDB 10.11 (сборка 10.11.13)
CentOS Stream 10	PostgreSQL 18 MariaDB 10.11 (сборка 10.11.13)

Первоначальная установка экземпляра Kaspersky Security Center Linux с использованием скрипта быстрой установки состоит из следующих этапов:

1. Подготовка к развертыванию

До начала действий по установке необходимо подготовить:

- Установочный образ диска операционной системы и репозиторий пакетов приложений.
- Приложение-аутентификатор для использования двухфакторной аутентификации (2FA) при входе в Web Console.
- Новый адрес FQDN (например, *ksclinux.example.com*). Вы можете использовать свой сценарий с присвоением прежнего адреса FQDN новому серверу при установке, если обладаете достаточным опытом настройки решений. В этом случае на шаге 5 "Настройка приложения после восстановления из резервной копии" пропустите этап 4. "Восстановление подключения управляемых устройств по адресу FQDN предыдущего Сервера администрирования".
- Устройство администратора с браузером для выхода в интернет для загрузки дистрибутивов и управления Web Console.
- Обеспечить доступность DNS и Сервера времени (NTP) для компонентов приложения.
- В зависимости от сценария освободить прежний IP-адрес, если для подключения управляемых устройств использовался IP-адрес.
- Настроить сетевое оборудование и прокси-сервер в соответствии с требованиями:
  - Порты для взаимодействия компонентов приложения.
  - Доступ к серверам "Лаборатории Касперского".
  - Рекомендации по Усилению защиты.

2. Выбор конфигурации и настройка операционной системы

1. Сконфигурируйте оборудование в зависимости от количества устройств, которыми будет управлять Сервер администрирования.

   Каждый расчет включает значения доступных ресурсов для работы приложений "Лаборатории Касперского". В расчет входит одновременная работа Сервера администрирования, Агента администрирования, СУБД, Сервера Web Console и Kaspersky Security Center Linux на одном устройстве. В расчет не входит хранение резервных копий Сервера администрирования.

Используйте внешний файловый ресурс в качестве точки монтирования для хранения резервных копий на отдельном устройстве, либо увеличьте свободное место на жестком диске с учетом хранения резервных копий.

Рекомендуется добавить дополнительные 4–6 ГБ оперативной памяти и 20 ГБ свободного места на жестком диске для работы операционной системы.

Расчет ресурсов устройства в зависимости от управляемых устройств:

- **S** (до 1000 устройств): CPU – 8 ядер, 16 ГБ оперативной памяти, 70 ГБ свободного места на жестком диске для директории `/var`, 300 IOPS или выше.
- **M** (до 10 000 устройств): CPU – 12 ядер, 24 ГБ оперативной памяти, 340 ГБ свободного места на жестком диске для директории `/var`, 300 IOPS или выше.
- **L** (до 30 000 устройств): CPU – 20 ядер, 40 ГБ оперативной памяти, 490 ГБ свободного места на жестком диске для директории `/var`, 300 IOPS или выше.
- **XL** (до 50 000 устройств): CPU – 28 ядер, 54 ГБ оперативной памяти, 640 ГБ свободного места на жестком диске для директории `/var`, 300 IOPS или выше.

2. Подготовьте оборудование для сервера Kaspersky Security Center Linux в соответствии с выбранными характеристиками.

3. Установите операционную систему на сервер Kaspersky Security Center Linux.

   При установке включите опцию **Средства удаленного подключения SSH**, если планируете управлять устройством Сервера администрирования с помощью удаленной командной строки.

   Astra Linux должна быть установлена без включенной опции **Мандатное управление доступом**. Также для правильной работы Kaspersky Endpoint Security для Linux требуется отключить опцию **Запрет трассировки ptrace**.

4. Проверьте доступное пространство для директории `/var`, если она смонтирована отдельно, либо для корневой директории `/`.

   Примеры для конфигурации M:

   Astra Linux

   ```
   administrator@ksclinux:~$ df -h
   Filesystem                Size  Used Avail Use% Mounted on
   /dev/mapper/astra48242-01  406G  8,0G 377G    3% /
   <...>
   ```

   Ubuntu

   ```
   administrator@ksclinux:~$ df -h
   Filesystem                         Size  Used Avail Use% Mounted on
   /dev/mapper/ubuntu--vg-ubuntu--lv  406G   11G  374G   3% /
   <...>
   ```

5. Настройте IP-адрес от прежнего Сервера администрирования на новом сервере, если для подключения управляемых устройств использовался IP-адрес.

Видео: настройка операционной системы{[Start_Delete_en-US]}



{[End_Delete_en-US]}



3. Загрузка файлов дистрибутива

1. Загрузите дистрибутивы нужной локализации с сайта "Лаборатории Касперского" и сохраните их в отдельную директорию (например, *kscdistr*).

   Для Ubuntu и Astra Linux

   - Дистрибутив deb Сервера администрирования:
     `Version 17.0.0.3992 | Debian x64 | Administration server`
   - Дистрибутив deb Web Console:
     `Version 17.0.14522 | Debian x64 | Web console`
   - Скрипт быстрой установки:
     `Version 17.0.0.3992 | Linux | KSC installation script`

   Для CentOS и РЕД ОС

   - Дистрибутив rpm Сервера администрирования:
     `Version 17.0.0.3992 | Red Hat Enterprise Linux x64 | Administration server`

- Дистрибутив rpm Web Console:

  `Version 17.0.14522 | Red Hat Enterprise Linux x64 | Web console`

- Скрипт быстрой установки:

  `Version 17.0.0.3992 | Linux | KSC installation script`

2. Для работы приложений "Лаборатории Касперского" в режиме Замкнутой программной среды (ЗПС) ОС Astra Linux скачайте файл публичного ключа kaspersky_astra_pub_key.gpg.

3. Скопируйте загруженные файлы на новое устройство с Сервером администрирования Kaspersky Security Center Linux с помощью съемного носителя или по сети.

   Ниже представлены действия, выполняемые в командной строке для копирования по сети.

   > Возможность использования утилиты scp для копирования зависит от наличия установленного запущенного сервиса SSH на стороне операционной системы устройства с Сервером администрирования и параметров безопасности вашей организации.

   a. В командной строке с помощью утилиты cd перейдите в директорию выше на один уровень директории *kscdistr*, например:

   Для Linux

   ```
   cd /home/administrator/Desktop
   ```

   Для Windows

   ```
   cd C:\Users\Administrator\Downloads
   ```

   b. Скопируйте файлы дистрибутива по сети с помощью утилиты scp:

   ```
   scp -r <kscdistr> <administrator>@<ksclinux.example.com>:
   ```

   где:

   `<kscdistr>` – локальная директория со скачанными дистрибутивами Kaspersky Security Center Linux;

   `<administrator>` – привилегированный пользователь на новом Сервере администрирования с правами подключения по протоколу SSH;

   `<ksclinux.example.com>` – FQDN-адрес нового Сервера администрирования.

   Файлы будут скопированы в корень директории профиля, указанного для подключения пользователя.

4. Настройка параметров установки

1. На новом устройстве с Сервером администрирования выполните вход под привилегированным пользователем и запустите командную строку.

2. Перейдите в директорию со скопированными дистрибутивами.

Пример

```
cd ~/kscdistr
```

3. Распакуйте архив скрипта быстрой установки в текущую директорию с файлами дистрибутивов.

Пример

```
tar -xf ./ksc_fast_install.tar.gz
```

4. Проверьте наличие всех файлов, выполнив команду:

```
ls -la
```

Пример вывода команды ls -la

```
administrator@ksclinux:~$ ls -la
drwxr-xr-x  3 administrator administrator      4096 oct 17 20:32 .
drwx------ 17 administrator administrator      4096 oct 17 17:54 ..
-rw-r--r--  1 administrator administrator       493 oct 20  2023 kaspersky_astra_pub_key.gpg
-rw-r--r--  1 administrator administrator 199128488 oct 10 21:38 ksc64_17.0.0-3992_amd64.deb
-rwxr-xr--  1 administrator administrator    143288 oct 22 17:22 ksc_fast_install.py
-rw-r--r--  1 administrator administrator 158144492 oct 10 21:37 ksc-web-console-17.0.14522.x86_64.deb
-rw-r--r--  1 administrator administrator     15561 oct 22 23:17 nwc_license.txt
-rw-r--r--  1 administrator administrator        64 oct 22 23:17 nwc_license.txt.sha256
-rw-r--r--  1 administrator administrator       493 oct 22 17:22 params.txt
-rw-r--r--  1 administrator administrator     70869 oct 22 23:17 server_license.txt
-rw-r--r--  1 administrator administrator        64 oct 22 23:17 server_license.txt.sha256
```

5. В директории с дистрибутивами откройте на редактирование текстовый файл параметров скрипта установки, например:

```
nano ./params.txt
```

6. Задайте подготовленные ранее значения и удалите первый символ комментирования (#) в нужных строках, либо добавьте новые строки со следующими значениями:

   - Расчетная конфигурация характеристик оборудования (доступные значения S/M/L/XL).

     Пример

     ```
     klfi_netsize=S
     ```

   - FQDN-адрес Сервера администрирования в двух параметрах файла.

     ```
     klfi_klserver_address=ksclinux.example.com
     ```

     ```
     klfi_kliam_address=ksclinux.example.com
     ```

Язык установленного Сервера администрирования зависит от локализации загруженного дистрибутива.

7. Проверьте правильность преобразования FQDN-адреса Сервера администрирования в петлевой (loopback) IP-адрес в операционной системе нового Сервера администрирования. Для этого:

   a. Выполните команду `ping` с адресом нового Сервера администрирования.

   Пример успешного получения петлевого IP-адреса

   ```
   administrator@ksclinux:~$ ping ksclinux.example.com
   ping ksclinux.example.com
   PING ksclinux.example.com (127.0.1.1) 56(84) bytes of data.
   64 bytes from ksclinux.example.com (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
   ```

   b. Добавьте адрес Сервера администрирования в файл `/etc/hosts` операционной системы нового Сервера администрирования, если адрес не был получен или получен внешний IP-адрес.

   Для этого:

   - Откройте файл `/etc/hosts` на редактирование, выполнив команду:

     ```
     sudo nano /etc/hosts
     ```

   - Введите адрес сервера в качестве FQDN-адреса устройства Сервера администрирования, например:

     ```
     127.0.0.1       localhost
     127.0.1.1       ksclinux.example.com ksclinux
     <...>
     ```

> На управляемых устройствах FQDN-адрес Сервера администрирования должен преобразовываться во внешний IP-адрес сервера. Обеспечьте правильную настройку записей на DNS серверах.

5. Запуск скрипта быстрой установки

{[Start_Delete_en-US]}В случае использования режима замкнутой программной среды (ЗПС) в ОС Astra Linux необходимо:

- Использовать максимальный уровень целостности (Высокий – уровень 63) для пользователя, под которым выполняется установка в операционной системы Astra Linux с задействованным механизмом **Мандатный контроль целостности**.

- Выполнить дополнительные шаги:

  1. Перейдите в директорию со скопированными дистрибутивами, например:

     ```
     cd ~/kscdistr
     ```

  2. Создайте директорию для размещения файла публичного ключа в системной директории:

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

3. Переместите файл публичного ключа `kaspersky_astra_pub_key.gpg` в системную директорию:

```
sudo mv ./kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
```

4. Установите пакет совместимости:

```
sudo apt install -y astra-digsig-oldkeys
```

5. Обновите загрузочный образ системы:

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

6. Перезагрузите операционную систему:

```
sudo reboot
```

{[End_Delete_en-US]}

Чтобы запустить скрипт быстрой установки:

1. После перезагрузки устройства вернитесь в директорию с дистрибутивами:

```
cd ~/kscdistr
```

2. Назначьте права выполнения для файла скрипта быстрой установки командой:

```
chmod +x ./ksc_fast_install.py
```

3. Ознакомьтесь с текстами условий Лицензионных соглашений вашей локализации до запуска скрипта, так как текст скрипта быстрой установки доступен только на английском языке.

4. Подключите сетевые репозитории пакетов в ОС или установочный образ диска ОС для скачивания пакетов во время установки.

5. Запустите скрипт быстрой установки:

```
sudo ./ksc_fast_install.py
```

6. Следуйте шагам мастера установки.

Если на шаге определения доступных ресурсов скрипт ошибочно определяет, что объем доступной оперативной памяти недостаточный, отключите использование оперативной памяти в динамическом режиме на время установки.

7. Дождитесь успешного завершения установки. Из текстового вывода скрипта сохраните имя пользователя (`User`) и пароль (`Pass`) для входа в Web Console.

Пример

```
[+] Creating KSC user 'kscadmin' ...
[+] An internal user has been created:
[+]     User: kscadmin
[+]     Pass: ############
[!] If the password is lost, you must create a user by running the command:
        /opt/kaspersky/ksc64/sbin/kladduser -n <user>
[+] OK
[+] Success
```

{[Start_Delete_en-US]}*Видео: Запуск скрипта быстрой установки для Astra Linux*



{[End_Delete_en-US]}

Видео: Запуск скрипта быстрой установки для Ubuntu



6. Первый вход в Web Console

1. В браузере откройте адрес для подключения к Web Console: `https://<FQDN>:8080`

   где `<FQDN>` – это адрес Сервера администрирования из параметров установки скрипта, например, *https://ksclinux.example.com:8080*.

2. Для входа в Web Console используйте имя пользователя и пароль из вывода скрипта.

3. Настройте приложение-аутентификатор:

   a. Скопируйте в приложение секретный ключ для получения одноразовых кодов подтверждений или отсканируйте QR-код из мастера настройки аутентификации Web Console.

   b. Введите сгенерированный код подтверждения для проверки и входа в Web Console.

4. Ознакомьтесь и подтвердите ознакомление с Руководством по усилению защиты.

5. Выполните настройку Сервера администрирования в Мастере первоначальной настройки, если не планируете восстановить данные Сервера администрирования из резервной копии.

4 Восстановление резервной копии Сервера администрирования

В сценариях миграции с Kaspersky Security Center Windows и в случае переноса данных Kaspersky Security Center Linux на новое оборудование может потребоваться восстановить резервную копию от предыдущей установки Сервера администрирования.

> Версия СУБД нового сервера должна быть не ниже версии в резервной копии.

Пропустите этот шаг, если восстановление данных не требуется.

Если создание резервной копии не было выполнено ранее:

- Создайте резервную копию предыдущей установки Сервера администрирования.

  Тип формата данных СУБД должен соответствовать новой установке.

- Установите новый сервер Kaspersky Security Center Linux и выполните первый вход в Web Console.

Восстановление резервной копии Сервера администрирования состоит из следующих этапов:

1. Перенос резервной копии на Сервер администрирования

Перенесите резервную копию предыдущего Сервера администрирования на новое устройство с Сервером администрирования с помощью съемного носителя или по сети.

Чтобы перенести резервную копию на Сервер администрирования по сети:

Возможность использования утилиты scp для копирования зависит от наличия установленного запущенного сервиса SSH на стороне операционной системы устройства с Сервером администрирования и параметров безопасности вашей организации.

1. В командной строке на устройстве с помощью утилиты *cd* перейдите в директорию, в которой расположена директория с файлами резервной копии предыдущего Сервера администрирования, например:

   Windows

   ```
   cd C:\kscbackups
   ```

   Linux

   ```
   cd /root/kscbackups
   ```

2. Выполните копирование директории с файлами резервной копии с помощью утилиты scp:

   ```
   scp -r <klbackup202x-xx-xx> <administrator>@<ksclinux.example.com>:
   ```

   где:

   `<klbackup202x-xx-xx>` – директория с непосредственно файлами резервной копии;

   `<administrator>` – привилегированный пользователь на новом Сервере администрирования с правами подключения по протоколу SSH;

   `<ksclinux.example.com>` – FQDN-адрес нового Сервера администрирования.

Директория с резервной копией будет скопирована в корень директории профиля указанного пользователя.

2. Процедура восстановления резервной копии

1. На новом устройстве с Сервером администрирования откройте командную строку.

2. Если в качестве СУБД используется PostgreSQL, на время восстановления данных из резервной копии предоставьте права суперпользователя PostgreSQL для стандартных учетных записей klserver и kliam, которые Сервер администрирования использует для подключения к СУБД:

   ```
   sudo -i -u postgres psql -c "ALTER ROLE klserver WITH SUPERUSER;"
   ```

   ```
   sudo -i -u postgres psql -c "ALTER ROLE kliam WITH SUPERUSER;"
   ```

3. С помощью утилиты klbackup запустите восстановление данных из резервной копии предыдущего Сервера администрирования:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klbackup -path </home/administrator/klbackup202x-xx-xx> -restore
   ```

   где `</home/administrator/klbackup202x-xx-xx>` – полный путь к директории с непосредственно файлами резервной копии.

4. Если пароль на резервную копию не был задан, в запросе пароля от резервной копии нажмите клавишу **Enter** без ввода пароля.

5. Дождитесь окончания работы утилиты.

   В крупных инсталляциях может требоваться значительное время.

6. Если в качестве СУБД используется PostgreSQL, восстановите исходные права у учетных записей PostgreSQL, которые Сервер администрирования использует для подключения к СУБД.

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH NOSUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH NOSUPERUSER;"
```

5 Настройка приложения после восстановления из резервной копии

Пропустите этот шаг, если вы не восстанавливали данные из резервной копии.

Настройка приложения после восстановления из резервной копии состоит из следующих этапов:

1. Восстановление работы Web Console

1. Получите значение адреса прежнего сервера из конфигурационного файла Сервера IAM:

```
sudo grep "ksc_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Пример

```
ksc_address: "oldksc.example.internal"
```

2. Проверьте правильность преобразования FQDN-адреса прежнего Сервера администрирования в петлевой (loopback) IP-адрес нового Сервера администрирования. Для этого:

   a. Выполните команду `ping` с адресом прежнего Сервера администрирования.

   Пример успешного получения петлевого IP-адреса

```
administrator@ksclinux:~$ ping oldksc.example.internal
ping oldksc.example.internal
PING ksclinux (127.0.1.1) 56(84) bytes of data.
64 bytes from ksclinux (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
```

   b. Добавьте адрес прежнего Сервера администрирования в файл `/etc/hosts` ОС нового Сервера администрирования, если адрес не был получен или получен внешний IP адрес. Для этого:

   - Откройте /etc/hosts на редактирование:

```
sudo nano /etc/hosts
```

- Введите имя прежнего сервера в качестве дополнительного псевдонима адреса устройства Сервера администрирования.

  Пример

  ```
  127.0.0.1       localhost
  127.0.1.1       ksclinux.example.com ksclinux oldksc.example.internal
  <...>
  ```

2. Восстановление доступа пользователя kscadmin для перехода с Kaspersky Security Center Windows

База пользователей была перезаписана, повторите создание пользователя kscadmin и настройку двухфакторной аутентификации.

1. Откройте командную строку в операционной системе устройства с Сервером администрирования, выполните команду создания пользователя:

   ```
   sudo /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin
   ```

   После нажатия **Enter** задайте пароль, затем повторите его.

2. В браузере откройте адрес для подключения к Web Console:

   ```
   https://<FQDN>:8080
   ```

   где `<FQDN>` – это адрес Сервера администрирования из параметров установки скрипта, например, *https://ksclinux.example.com:8080*.

3. Используйте созданные имя пользователя и пароль для входа в Web Console.

4. Настройте приложение-аутентификатор. Для этого:

   a. Удалите устаревший профиль учетной записи пользователя kscadmin, который был настроен в приложении-аутентификаторе до восстановления резервной копии Сервера администрирования.

   b. Скопируйте в приложение секретный ключ для получения одноразовых кодов подтверждений или отсканируйте QR-код из мастера настройки аутентификации Web Console.

   c. Введите сгенерированный код подтверждения для проверки и входа в Web Console.

3. Проверка работы Сервера администрирования

1. Проверьте работоспособность интерфейса Web Console под пользователем kscadmin и другими пользователями.

2. Последовательно запустите следующие задачи:

   - Загрузка обновлений в хранилище Сервера администрирования.
   - Обслуживание Сервера администрирования.
   - Резервное копирование данных Сервера администрирования.

Замените Windows-пути в параметрах задач на Linux-директории нового Сервера администрирования, либо удалите и сконфигурируйте задачи повторно.

3. Проверьте результат выполнения задач и если необходимо, внесите изменения в параметры работы задач, политик управления и настроек Сервера администрирования.

4. Восстановление подключения управляемых устройств по адресу FQDN предыдущего Сервера администрирования

Если вы присвоили новый адрес FQDN новому Серверу администрирования (например, ksclinux.example.com), добавьте один из следующих типов записей DNS:

- Запись CNAME, связывающая старое имя Сервера администрирования с новым именем Сервера администрирования.

  Дополнительную информацию о настройке требуемых записей см. в документации DNS-сервера.

- Запись A и AAAA для прежнего адреса Сервера администрирования, указывающая на новый IP-адрес Сервера администрирования.

  Для службы DNS на базе Windows Server выполняйте команды с использованием значений, применимых к вашей инфраструктуре.

Чтобы добавить DNS-запись A для службы DNS на базе Windows Server выполняйте команды с использованием значений, применимых к вашей инфраструктуре:

1. Подключитесь к DNS-серверу.

2. Откройте PowerShell и получите IP-адрес из существующей записи A, выполнив команду:

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

3. Измените IP-адрес в A-записи, выполнив команды:

```
$OldKSC = Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

```
$NewKSC = $OldKSC.Clone()
```

```
$NewKSC.RecordData.IPv4Address = [System.Net.IPAddress]::parse('<IP address of the administration server>')
```

```
Set-DnsServerResourceRecord -OldInputObject $OldKSC -NewInputObject $NewKSC -ZoneName "<zone name>"
```

4. Убедитесь, что IP-адрес в записи A обновлен, выполнив команду:

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

В выводе команды отобразится IP-адрес сервера администрирования Kaspersky Security Center Linux. Управляемые устройства восстановят подключение после обновления локального кеша DNS.

6 Настройка антивирусной защиты Сервера администрирования

Чтобы выполнить рекомендации по усилению защиты в части обеспечения Сервера администрирования антивирусной защитой, установите приложения "Лаборатории Касперского" на Сервер администрирования и настройте политики управления. Для развертывания Kaspersky Endpoint Security для Linux используйте руководство по развертыванию.

Установка и настройка состоит из следующих этапов:

1. Создание отдельной группы администрирования

1. В главном окне Web Console выберите **Управление активами** → **Иерархия групп**.
2. Установите флажок рядом с группой **Управляемые устройства**.
3. Нажмите на кнопку **Добавить**.
4. В открывшемся окне укажите имя новой группы (например, *kscserver*) и подтвердите ее создание нажатием на кнопку **Добавить**.

2. Создание политики для Агента администрирования без наследования параметров

1. В главном окне Web Console перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на кнопку **Добавить**.
3. В Мастере создания новой политики выберите приложение **Агент администрирования Kaspersky Security Center Linux** и нажмите **Далее**.
4. Отключите опцию **Наследовать параметры родительской политики** и нажмите **Сохранить**.

3. Установка плагина управления Kaspersky Endpoint Security для Linux из Kaspersky Security Center или вручную

Вы можете установить плагин управления Kaspersky Endpoint Security для Linux следующими способами:

- Установка из списка доступных дистрибутивов в разделе **Каталог приложений "Лаборатории Касперского"** в Web Console.
- Установка вручную из файла.

Чтобы установить плагин управления Kaspersky Endpoint Security из списка доступных дистрибутивов в Web Console:

1. В главном окне Web Console выберите **Параметры** → **Веб-плагины**.

   Откроется список установленных веб-плагинов.

2. Нажмите на кнопку **Добавить**.

   Откроется список доступных плагинов управления. Список обновляется автоматически после выпуска новых версий веб-плагинов.

3. В списке доступных плагинов выберите последнюю доступную версию веб-плагина Kaspersky Endpoint Security для Linux.

4. В открывшемся окне с описанием веб-плагина нажмите на кнопку **Установить плагин**.

5. Дождитесь окончания установки и нажмите на кнопку **OK** в информационном окне.

Новый плагин отобразится в списке установленных веб-плагинов.

Видео: установка веб-плагина управления с помощью мастера



Чтобы установить плагин управления Kaspersky Endpoint Security вручную из файла:

1. Скачайте архив с веб-плагином на странице загрузки приложений в разделе Kaspersky Endpoint Security для Linux: **Плагин контроля приложений → Web console Plug-In**.

2. Локально распакуйте скачанный архив.

3. В главном окне Web Console выберите **Параметры → Веб-плагины**.

   Откроется список установленных веб-плагинов.

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

5. В открывшемся окне укажите путь к файлу plugin.zip и путь к файлу signature.txt.

   Файлы находятся в папке, куда вы распаковали архив с веб-плагином.

6. Нажмите на кнопку **Добавить**.

7. Дождитесь окончания установки и нажмите на кнопку **OK** в информационном окне.

Новый плагин отобразится в списке установленных веб-плагинов (**Параметры → Веб-плагины**).

Видео: установка веб-плагина управления в изолированных сетях



4. Создание политики для Kaspersky Endpoint Security для Linux без наследования параметров

При совместной работе Kaspersky Endpoint Security для Linux и Kaspersky Security Center Linux вам нужно настроить параметры политики в соответствии с рекомендациями специалистов "Лаборатории Касперского".

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Выберите группу администрирования для Сервера администрирования.
3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания политики.
4. В открывшемся окне в списке выберите название приложения Kaspersky Endpoint Security для Linux.
5. Укажите **Стандартный режим или режим Агента Endpoint Detection and Response** приложения Kaspersky Endpoint Security для Linux.
6. Примите решение об использовании Kaspersky Security Network.
7. Ознакомьтесь с рекомендациями по оптимизации для управляемых устройств.
8. В названии политики укажите принадлежность политики к Серверу администрирования.
9. Отключите опцию **Наследовать параметры родительской политики**.
10. Сохраните внесенные изменения.

Видео: создание политики



5. Создание групповой задачи Обновление для Kaspersky Endpoint Security для Linux

1. В главном окне Web Console выберите раздел **Задачи**.
2. Выберите группу администрирования для Сервера администрирования.
3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задач.
4. В открывшемся окне в списке выберите название приложения Kaspersky Endpoint Security для Linux.
5. Укажите тип задачи *Обновление* и пройдите следующие шаги без изменения параметров.

   Запустится окно свойств задачи.
6. В разделе **Параметры приложения** → **Источники обновлений** включите источник Kaspersky Security Center и поднимите его приоритет.

В изолированных сетях используйте утилиту Kaspersky Update Utility для формирования хранилища для задач обновления.

Видео: настройка централизованного обновления баз



6. Добавление лицензионного ключа в хранилище Сервера администрирования с функцией автоматического распространения

1. В главном окне Kaspersky Security Center Web Console выберите раздел **Лицензии**.
2. Нажмите на кнопку **Добавить**.
3. Укажите опцию **Код активации** и нажмите **Отправить**.

   В изолированных сетях используйте файл ключа, который можно запросить с помощью сервиса https://keyfile.kaspersky.com/ru-RU.
4. В списке лицензий нажмите на название лицензии.
5. Установите флажок **Автоматически распространять лицензионный ключ на управляемые устройства**.
6. Сохраните изменения.

Видео: активация приложения с помощью кода активации



Видео: активация приложения с помощью файла ключа



7. Создание инсталляционных пакетов Агента администрирования и Kaspersky Endpoint Security для Linux

1. В главном окне Web Console выберите **Управление программным обеспечением → Инсталляционные пакеты**.
2. Нажмите на кнопку **Добавить**.

   Запустится Мастер создания инсталляционного пакета.
3. Выберите **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**.
4. В списке приложений найдите последнюю версию Kaspersky Endpoint Security для Linux и нажмите на название.
5. В боковой панели инициируйте загрузку кнопкой **Скачать и создать инсталляционный пакет**.

   Ознакомьтесь и примите лицензионные соглашения для начала использования приложений.
6. Вернитесь в список приложений и загрузите последнюю версию Агента администрирования (Kaspersky Network Agent for Linux).

   Ознакомьтесь и примите лицензионные соглашения для начала использования приложений.
7. В главном окне Web Console в списке загруженных приложений нажмите на названия приложений.

В изолированных сетях скачайте дистрибутивы с сайта "Лаборатории Касперского" и выберите в Мастере создания инсталляционного пакета опцию **Создать инсталляционный пакет из файла**.

Видео: создание инсталляционного пакета автоматически в Kaspersky Security Center



Видео: создание инсталляционного пакета вручную из файла в Kaspersky Security Center



8. Установка Агента администрирования для Linux

1. В главном окне Web Console выберите **Управление программным обеспечением → Инсталляционные пакеты**.
2. Установите флажок напротив пакета **Агента администрирования (Kaspersky Network Agent for Linux)**.
3. Нажмите **Развернуть**.

   Запустится Мастер развертывания защиты.
4. Выберите вариант **С использованием автономного инсталляционного пакета**.
5. На шаге **Перемещение устройств в папку Управляемые устройства** пропустите настройку правил перемещения устройств в группу администрирования. Эта опция не применяется для устройства Сервера администрирования.
6. На шаге **Результат формирования автономного инсталляционного пакета** выделите и скопируйте полный путь размещения скрипта установки приложения.
7. В операционной системе Сервера администрирования откройте командную строку.
8. Запустите установку автономного пакета:

   ```
   sudo bash "</var/opt/.../stand-alone_package_sh>"
   ```

   где `</var/opt/.../stand-alone_package_sh>` – это ранее скопированный полный путь к файлу скрипта автономного инсталляционного пакета приложения.

   В случае успешной установки отобразится соответствующее уведомление.
9. Переместите устройство Сервера администрирования (например, *ksclinux*) из группы **Управляемые устройства** в ранее подготовленную группу администрирования (например, *kscserver*).

9. Установка Kaspersky Endpoint Security для Linux

1. В главном окне Web Console выберите **Управление программным обеспечением → Инсталляционные пакеты**.
2. Установите флажок напротив пакета Kaspersky Endpoint Security для Linux.

3. Нажмите **Развернуть**.

   Запустится Мастер развертывания защиты.

4. Выберите вариант **С использованием автономного инсталляционного пакета**.

5. На шаге **Результат формирования автономного инсталляционного пакета** выделите и скопируйте полный путь размещения скрипта установки приложения.

6. В операционной системе Сервера администрирования откройте командную строку.

7. Запустите установку автономного пакета:

   ```
   sudo bash "</var/opt/.../stand-alone_package_sh>"
   ```

   где `</var/opt/.../stand-alone_package_sh>` – это ранее скопированный полный путь к файлу скрипта автономного инсталляционного пакета приложения.

   В случае успешной установки отобразится соответствующее уведомление.

8. В главном окне Web Console в разделе **Задачи** выберите корневой узел в списке групп администрирования с названием Сервера администрирования.

9. Из списка задач Сервера администрирования последовательно запустите следующие задачи:

   - Загрузка обновлений в хранилище Сервера администрирования.
   - Обновление (Kaspersky Endpoint Security для Linux).

10. В главном окне Web Console выберите **Управление активами** → **Управляемые устройства**.

11. Нажмите на имя объекта устройства Сервера администрирования.

12. Проверьте значения основных показателей состояния устройства:

    - Последнее обновление антивирусных баз (актуально).
    - Подключено к Серверу администрирования (актуально).
    - Состояние защиты (Выполняется).
    - Событие *Ключ успешно добавлен* (есть).

Используйте руководство по развертыванию Kaspersky Endpoint Security для Linux для развертывания приложения на устройствах сети.

Общее руководство по миграции на новый сервер Kaspersky Security Center Linux

Вы можете использовать резервную копию данных для переноса данных Сервера администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux на новый сервер Kaspersky Security Center Linux при миграции решения или переноса для замены оборудования.

Перед переносом данных с Kaspersky Security Center Windows убедитесь, что необходимые функции Kaspersky Security Center Windows поддерживаются в Kaspersky Security Center Linux.

Общее руководство по миграции рассматривает сценарий, когда новый Сервер администрирования будет иметь новое DNS-имя. Для восстановления подключения управляемых устройств необходимо изменить запись DNS прежнего сервера. Вы можете использовать свой сценарий с присвоением прежнего адреса новому серверу при установке, если обладаете достаточным опытом настройки решений. Нахождение в сети прежнего Сервера администрирования может вызывать сбои управления устройствами и нарушение входа в Web Console нового Сервера администрирования, а также запуск задачи установки Агента администрирования с подключением к старому серверу.

Ограничения

- Перенос данных возможен между следующими СУБД:
  - Microsoft SQL Server → MySQL, MariaDB.
  - Microsoft SQL Server → PostgreSQL, Postgres Pro.
  - MySQL → MySQL, MariaDB.
  - MariaDB → MySQL, MariaDB.
  - PostgreSQL → PostgreSQL.
  - Postgres Pro → Postgres Pro.
- Необходимо задать целевой тип СУБД в утилите резервного копирования при переходе с Microsoft SQL Server, в остальных сценариях переноса совместимость баз определяется пунктом выше.
- Версия СУБД нового Сервера администрирования должна быть не ниже версии СУБД, используемой на прежнем Сервере администрирования.
- Kaspersky Security Center Windows должен быть обновлен до последней версии перед созданием резервной копии для переноса данных.
- Если вы используете MySQL или MariaDB в качестве СУБД для Kaspersky Security Center Windows и для Kaspersky Security Center Linux, параметр `lower_case_table_names` должен совпадать в текущей и новой СУБД.

1 Предварительные действия перед созданием резервной копии

Этот шаг содержит инструкции по подготовке ранее настроенного Сервера администрирования для дальнейшей миграции на новый Сервер администрирования Kaspersky Security Center Linux. Подготовка состоит из следующих этапов:

1. Проверка версии Сервера администрирования для создания совместимой с Kaspersky Security Center Linux резервной копии.

Все актуальные версии **Kaspersky Security Center Linux** поддерживают перенос данных с обновлением на более новую версию приложения. Создание и восстановление резервных копий возможно только в рамках одного типа СУБД.

Для **Kaspersky Security Center Windows** необходимо проверить версию Сервера администрирования в **Свойства** → **Общие** → **Версия**. Если версия ниже, чем 15.1.0.28509, обновите Kaspersky Security Center Windows до последней версии.

Обновление Kaspersky Security Center Windows до последней версии

1. На сайте "Лаборатории Касперского" скачайте дистрибутив, соответствующий языку локализации установленного Сервера администрирования: `Version 15.1.0.28509 | Windows | Full distributive`.

   Исполняемый файл сохраняется в папку **Загрузки** со следующим названием: `ksc_15.1_<build number>_full_<language>.exe`.

2. Скопируйте дистрибутив на Сервер администрирования.

3. Запустите от администратора исполняемый файл `ksc_15.1_<build number>_full_<language>.exe`.

4. В открывшемся окне нажмите на ссылку **Установить Kaspersky Security Center**.

   Запустится мастер установки Сервера администрирования.

5. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения следующих документов** установите флажки:

   - **Условия и положения настоящего Лицензионного соглашения**.
   - **Политику конфиденциальности, которая описывает обработку данных**.

6. Выберите **Обновить Сервер администрирования и консоль на основе веб-интерфейса (рекомендуется)** и перейдите к следующему шагу.

7. Создайте новую резервную копию, выберите опцию **Я хочу создать резервную копию данных** и пройдите мастер создания резервной копии.

8. Нажмите **Обновить**.

9. Во время обновления в мастере установки Web Console подтвердите все шаги мастера для обновления версии.

   Процесс установки обновления Сервера администрирования займет некоторые время. После завершения мастера установки Консоль администрирования может не принимать подключения до завершения инициализации базы данных.

10. Дождитесь полного завершения процедуры обновления.

2. Проверка выполнения требований к сертификату Сервера администрирования.

   Перед созданием резервной копии вам нужно убедиться, что сертификат содержит альтернативное имя субъекта (Subject Alternative Name, SAN). Если нет, важно заменить сертификат, иначе вы не сможете войти в Web Console после восстановления из резервной копии.

Чтобы проверить, что сертификат включает альтернативное имя субъекта:

- Для устройств с операционной системой Windows:

  a. В Консоли администрирования выберите Сервер администрирования, для которого требуется проверка.

  b. В контекстном меню выберите пункт **Свойства** → **Общие** → **Просмотреть сертификат Сервера**.

  c. В открывшемся окне проверьте значение пункта **Альтернативное имя субъекта**.

- Для устройств с операционной системой Linux выполните команду:

```
sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
```

Убедитесь, что альтернативное имя субъекта содержит доменное имя (DNS) устройства Сервера администрирования.

Если значение содержит только IP-адрес в сети или значение полностью отсутствует, вручную замените сертификат на соответствующий требованиям работы с Kaspersky Security Center Linux. Замените общий сертификат Сервера администрирования с помощью утилиты klsetsrvcert.

Замена общего сертификата Сервера администрирования с помощью утилиты klsetsrvcert

1. Создайте новый сертификат с отложенной датой начала использования на устройствах, выполнив команду:

   - Для Kaspersky Security Center Windows:

```
"%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -t CR -g "
<oldksc.example.internal>" -o "RsaKeyLen:2048"
```

   - Для Kaspersky Security Center Linux:

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert -t CR -g "<oldksc.example.internal>" -o "RsaKeyLen:2048"
```

   где `"<oldksc.example.internal>"` – FQDN-адрес подключения к Серверу администрирования.

   > Не используйте IP-адрес для этого значения.

2. Назначьте дату начала использования нового сертификата на всех устройствах, выполнив команду:

   - Для Kaspersky Security Center Windows:

```
"%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -f "DD-MM-YYYY hh:mm"
```

   - Для Kaspersky Security Center Linux:

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert -f "DD-MM-YYYY hh:mm"
```

где дата `"DD-MM-YYYY hh:mm"` минимум на 30 дней больше текущей. По умолчанию период распространения нового сертификата (`CR`) составляет 90 дней.

> После наступления назначенного времени может потребоваться переустановить Web Console чтобы восстановить к ней доступ и актуализировать сертификат в ее составе.

3. Если необходимо, после миграции на новый Сервер администрирования запустите утилиту klmover, чтобы восстановить соединение устройств с Сервером администрирования. Запуск утилиты может понадобиться, если устройство было выключено весь период распространения сертификата или не подключалось к Серверу администрирования.

2 Создание резервной копии предыдущей установки Сервера администрирования

Создание резервной копии Kaspersky Security Center Windows

1. Из меню **Пуск** → **Kaspersky Security Center** → **Kaspersky Backup Utility** запустите утилиту `klbackup.exe`, расположенную в папке установки Kaspersky Security Center Linux.

   Запустится мастер установки. На ОС Microsoft Windows в режиме Server Core используйте консольную версию утилиты klbackup.

2. На первом шаге выберите **Выполнить резервное копирование данных Сервера администрирования**.

3. На шаге **Параметры резервного копирования** выполните следующие действия:

   a. Нажмите на кнопку **Обзор** и создайте новую папку для сохранения резервной копии отдельно от директории по умолчанию, например `C:\kscbackups`.

   b. Если вы используете Microsoft SQL Server, выберите опцию **Перенос базы данных** → **Перенести в формат Postgres** или **Перенос данных в формате MySQL/MariaDB**.

   Если используется не Microsoft SQL Server, в резервной копии сохранится прежний тип базы данных.

   c. Задайте пароль к резервной копии для защиты от несанкционированного доступа к данным.

4. Дождитесь создания резервной копии и завершите работу утилиты.

В директории создана новая директория с отметкой времени создания резервной копии.

Создание резервной копии Kaspersky Security Center Linux

1. На устройстве с Сервером администрирования в командной строке введите следующую команду:

```
sudo /opt/kaspersky/ksc64/sbin/klbackup -path /root/kscbackups -use_ts
```

2. Дождитесь завершения создания резервной копии.

В директории, указанной после параметра `-path`, будет создана новая директория с отметкой времени создания резервной копии.

После создания резервной копии предыдущего Сервера администрирования, выведите из эксплуатации устройство с Сервером администрирования.

Вывод устройства с Сервером администрирования из эксплуатации

1. Скопируйте полученную резервную копию для переноса данных на устройство администратора.
2. Завершите работу операционной системы Сервера администрирования.
3. Отключите сетевой адаптер от корпоративной сети.
4. Освободите IP-адрес устройства, если планируете использовать его для новой установки Kaspersky Security Center Linux.
5. Убедитесь, что устройство полностью отключено.

Нахождение в сети прежнего Сервера администрирования может вызывать сбои управления устройствами и нарушение входа в Web Console нового Сервера администрирования, а также запуск задачи установки Агента администрирования с подключением к старому серверу.

3 Первоначальная установка Kaspersky Security Center Linux

- **Подготовка к развертыванию**

  До начала действий по установке необходимо подготовить:

  - Установочный образ диска операционной системы и репозиторий пакетов приложений.
  - Приложение-аутентификатор для использования двухфакторной аутентификации (2FA) при входе в Web Console.
  - Новый адрес FQDN (например, *ksclinux.example.com*). Вы можете использовать свой сценарий с присвоением прежнего адреса FQDN новому серверу при установке, если обладаете достаточным опытом настройки решений. В этом случае на шаге 5 "Настройка приложения после восстановления из резервной копии" пропустите этап 4. "Восстановление подключения управляемых устройств по адресу FQDN предыдущего Сервера администрирования".
  - Устройство администратора с браузером для выхода в интернет для загрузки дистрибутивов и управления Web Console.
  - Обеспечить доступность DNS и Сервера времени (NTP) для компонентов приложения.
  - В зависимости от сценария освободить прежний IP-адрес, если для подключения управляемых устройств использовался IP-адрес.
  - Настроить сетевое оборудование и прокси-сервер в соответствии с требованиями:
    - Порты для взаимодействия компонентов приложения.
    - Доступ к серверам "Лаборатории Касперского".
    - Рекомендации по Усилению защиты.

- **Выбор конфигурации, настройка и установка**

  a. Подготовьте оборудование для Сервера администрирования, СУБД и Web Console в соответствии с аппаратными и программными требованиями и расчетными характеристиками оборудования для обеспечения управления необходимым количеством устройств с планируемой нагрузкой.

  Для повышения уровня защищенности компонентов решения включите в расчеты конфигураций и установите на узлы Kaspersky Security Center Linux приложение Kaspersky Endpoint Security для Linux.

  b. Установите и настройте ОС, компоненты решения Kaspersky Security Center в соответствии с инструкцией по первоначальному развертыванию решения.

- **Первый вход в Web Console**

  1. В браузере откройте адрес для подключения к Web Console: `https://<FQDN>:8080`

  где `<FQDN>` – это адрес Сервера администрирования из параметров установки скрипта, например, *https://ksclinux.example.com:8080*.

  2. Для входа в Web Console используйте имя пользователя и пароль из вывода скрипта.

  3. Настройте приложение-аутентификатор:

  a. Скопируйте в приложение секретный ключ для получения одноразовых кодов подтверждений или отсканируйте QR-код из мастера настройки аутентификации Web Console.

  b. Введите сгенерированный код подтверждения для проверки и входа в Web Console.

  4. Ознакомьтесь и подтвердите ознакомление с Руководством по усилению защиты.

  5. Выполните настройку Сервера администрирования в Мастере первоначальной настройки, если не планируете восстановить данные Сервера администрирования из резервной копии.

4 Восстановление резервной копии Сервера администрирования

Восстановление резервной копии Сервера администрирования состоит из следующих этапов:

1. Перенос резервной копии на Сервер администрирования

Перенесите резервную копию предыдущего Сервера администрирования на новое устройство с Сервером администрирования с помощью съемного носителя или по сети.

Чтобы перенести резервную копию на Сервер администрирования по сети:

Возможность использования утилиты scp для копирования зависит от наличия установленного запущенного сервиса SSH на стороне операционной системы устройства с Сервером администрирования и параметров безопасности вашей организации.

1. В командной строке на устройстве с помощью утилиты *cd* перейдите в директорию, в которой расположена директория с файлами резервной копии предыдущего Сервера администрирования, например:

   Windows

   ```
   cd C:\kscbackups
   ```

   Linux

   ```
   cd /root/kscbackups
   ```

2. Выполните копирование директории с файлами резервной копии с помощью утилиты scp:

   ```
   scp -r <klbackup202x-xx-xx> <administrator>@<ksclinux.example.com>:
   ```

   где:

   `<klbackup202x-xx-xx>` – директория с непосредственно файлами резервной копии;

   `<administrator>` – привилегированный пользователь на новом Сервере администрирования с правами подключения по протоколу SSH;

   `<ksclinux.example.com>` – FQDN-адрес нового Сервера администрирования.

Директория с резервной копией будет скопирована в корень директории профиля указанного пользователя.

2. Процедура восстановления резервной копии

1. На новом устройстве с Сервером администрирования откройте командную строку.

2. Если в качестве СУБД используется PostgreSQL, на время восстановления данных из резервной копии предоставьте права суперпользователя PostgreSQL для стандартных учетных записей klserver и kliam, которые Сервер администрирования использует для подключения к СУБД:

   ```
   sudo -i -u postgres psql -c "ALTER ROLE klserver WITH SUPERUSER;"
   ```

   ```
   sudo -i -u postgres psql -c "ALTER ROLE kliam WITH SUPERUSER;"
   ```

3. С помощью утилиты klbackup запустите восстановление данных из резервной копии предыдущего Сервера администрирования:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klbackup -path </home/administrator/klbackup202x-xx-xx> -restore
   ```

   где `</home/administrator/klbackup202x-xx-xx>` – полный путь к директории с непосредственно файлами резервной копии.

4. Если пароль на резервную копию не был задан, в запросе пароля от резервной копии нажмите клавишу **Enter** без ввода пароля.

5. Дождитесь окончания работы утилиты.

   В крупных инсталляциях может требоваться значительное время.

6. Если в качестве СУБД используется PostgreSQL, восстановите исходные права у учетных записей PostgreSQL, которые Сервер администрирования использует для подключения к СУБД.

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH NOSUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH NOSUPERUSER;"
```

5 Настройка приложения после восстановления из резервной копии

Пропустите этот шаг, если вы не восстанавливали данные из резервной копии.

Настройка приложения после восстановления из резервной копии состоит из следующих этапов:

1. Восстановление работы Web Console

1. Получите значение адреса прежнего сервера из конфигурационного файла Сервера IAM:

```
sudo grep "ksc_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Пример

```
ksc_address: "oldksc.example.internal"
```

2. Проверьте правильность преобразования FQDN-адреса прежнего Сервера администрирования в петлевой (loopback) IP-адрес нового Сервера администрирования. Для этого:

   a. Выполните команду `ping` с адресом прежнего Сервера администрирования.

   Пример успешного получения петлевого IP-адреса

```
administrator@ksclinux:~$ ping oldksc.example.internal
ping oldksc.example.internal
PING ksclinux (127.0.1.1) 56(84) bytes of data.
64 bytes from ksclinux (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
```

   b. Добавьте адрес прежнего Сервера администрирования в файл `/etc/hosts` ОС нового Сервера администрирования, если адрес не был получен или получен внешний IP адрес. Для этого:

   - Откройте /etc/hosts на редактирование:

```
sudo nano /etc/hosts
```

- Введите имя прежнего сервера в качестве дополнительного псевдонима адреса устройства Сервера администрирования.

  Пример

  ```
  127.0.0.1       localhost
  127.0.1.1       ksclinux.example.com ksclinux oldksc.example.internal
  <...>
  ```

2. Восстановление доступа пользователя kscadmin для перехода с Kaspersky Security Center Windows

База пользователей была перезаписана, повторите создание пользователя kscadmin и настройку двухфакторной аутентификации.

1. Откройте командную строку в операционной системе устройства с Сервером администрирования, выполните команду создания пользователя:

   ```
   sudo /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin
   ```

   После нажатия **Enter** задайте пароль, затем повторите его.

2. В браузере откройте адрес для подключения к Web Console:

   ```
   https://<FQDN>:8080
   ```

   где `<FQDN>` – это адрес Сервера администрирования из параметров установки скрипта, например, *https://ksclinux.example.com:8080*.

3. Используйте созданные имя пользователя и пароль для входа в Web Console.

4. Настройте приложение-аутентификатор. Для этого:

   a. Удалите устаревший профиль учетной записи пользователя kscadmin, который был настроен в приложении-аутентификаторе до восстановления резервной копии Сервера администрирования.

   b. Скопируйте в приложение секретный ключ для получения одноразовых кодов подтверждений или отсканируйте QR-код из мастера настройки аутентификации Web Console.

   c. Введите сгенерированный код подтверждения для проверки и входа в Web Console.

3. Проверка работы Сервера администрирования

1. Проверьте работоспособность интерфейса Web Console под пользователем kscadmin и другими пользователями.

2. Последовательно запустите следующие задачи:

   - Загрузка обновлений в хранилище Сервера администрирования.
   - Обслуживание Сервера администрирования.
   - Резервное копирование данных Сервера администрирования.

Замените Windows-пути в параметрах задач на Linux-директории нового Сервера администрирования, либо удалите и сконфигурируйте задачи повторно.

3. Проверьте результат выполнения задач и если необходимо, внесите изменения в параметры работы задач, политик управления и настроек Сервера администрирования.

4. Восстановление подключения управляемых устройств по адресу FQDN предыдущего Сервера администрирования

Если вы присвоили новый адрес FQDN новому Серверу администрирования (например, ksclinux.example.com), добавьте один из следующих типов записей DNS:

- Запись CNAME, связывающая старое имя Сервера администрирования с новым именем Сервера администрирования.

  Дополнительную информацию о настройке требуемых записей см. в документации DNS-сервера.

- Запись A и AAAA для прежнего адреса Сервера администрирования, указывающая на новый IP-адрес Сервера администрирования.

  Для службы DNS на базе Windows Server выполняйте команды с использованием значений, применимых к вашей инфраструктуре.

Чтобы добавить DNS-запись A для службы DNS на базе Windows Server выполняйте команды с использованием значений, применимых к вашей инфраструктуре:

1. Подключитесь к DNS-серверу.

2. Откройте PowerShell и получите IP-адрес из существующей записи A, выполнив команду:

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

3. Измените IP-адрес в A-записи, выполнив команды:

```
$OldKSC = Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

```
$NewKSC = $OldKSC.Clone()
```

```
$NewKSC.RecordData.IPv4Address = [System.Net.IPAddress]::parse('<IP address of the administration server>')
```

```
Set-DnsServerResourceRecord -OldInputObject $OldKSC -NewInputObject $NewKSC -ZoneName "<zone name>"
```

4. Убедитесь, что IP-адрес в записи A обновлен, выполнив команду:

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

В выводе команды отобразится IP-адрес сервера администрирования Kaspersky Security Center Linux. Управляемые устройства восстановят подключение после обновления локального кеша DNS.

6 Настройка антивирусной защиты Сервера администрирования

С целью выполнения рекомендаций по Усилению защиты в части обеспечения Сервера администрирования антивирусной защитой, выполните установку приложений "Лаборатории Касперского" на Сервер администрирования и настройку политик управления для установленных приложений.

Установка и настройка состоит из следующих этапов:

1. Создание отдельной группы администрирования

1. В главном окне Web Console выберите **Управление активами** → **Иерархия групп**.
2. Установите флажок рядом с группой **Управляемые устройства**.
3. Нажмите на кнопку **Добавить**.
4. В открывшемся окне укажите имя новой группы (например, *kscserver*) и подтвердите ее создание нажатием на кнопку **Добавить**.

2. Создание политики для Агента администрирования без наследования параметров

1. В главном окне Web Console перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на кнопку **Добавить**.
3. В Мастере создания новой политики выберите приложение **Агент администрирования Kaspersky Security Center Linux** и нажмите **Далее**.
4. Отключите опцию **Наследовать параметры родительской политики** и нажмите **Сохранить**.

3. Установка плагина управления Kaspersky Endpoint Security для Linux из Kaspersky Security Center Linux или вручную

Вы можете установить плагин управления Kaspersky Endpoint Security для Linux следующими способами:

- Установка из списка доступных дистрибутивов в разделе **Каталог приложений "Лаборатории Касперского"** в Web Console.
- Установка вручную из файла.

Чтобы установить плагин управления Kaspersky Endpoint Security из списка доступных дистрибутивов в Web Console:

1. В главном окне Web Console выберите **Параметры** → **Веб-плагины**.

   Откроется список установленных веб-плагинов.

2. Нажмите на кнопку **Добавить**.

   Откроется список доступных плагинов управления. Список обновляется автоматически после выпуска новых версий веб-плагинов.

3. В списке доступных плагинов выберите последнюю доступную версию веб-плагина Kaspersky Endpoint Security для Linux.

4. В открывшемся окне с описанием веб-плагина нажмите на кнопку **Установить плагин**.

5. Дождитесь окончания установки и нажмите на кнопку **OK** в информационном окне.

Новый плагин отобразится в списке установленных веб-плагинов.

Видео: установка веб-плагина управления с помощью мастера



Чтобы установить плагин управления Kaspersky Endpoint Security вручную из файла:

1. Скачайте архив с веб-плагином на странице загрузки приложений в разделе Kaspersky Endpoint Security для Linux: **Плагин контроля приложений → Web console Plug-In**.

2. Локально распакуйте скачанный архив.

3. В главном окне Web Console выберите **Параметры → Веб-плагины**.

   Откроется список установленных веб-плагинов.

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

5. В открывшемся окне укажите путь к файлу plugin.zip и путь к файлу signature.txt.

   Файлы находятся в папке, куда вы распаковали архив с веб-плагином.

6. Нажмите на кнопку **Добавить**.

7. Дождитесь окончания установки и нажмите на кнопку **OK** в информационном окне.

Новый плагин отобразится в списке установленных веб-плагинов (**Параметры → Веб-плагины**).

Видео: установка веб-плагина управления в изолированных сетях



4. Создание политики для Kaspersky Endpoint Security для Linux без наследования параметров

При совместной работе Kaspersky Endpoint Security для Linux и Kaspersky Security Center Linux вам нужно настроить параметры политики в соответствии с рекомендациями специалистов "Лаборатории Касперского".

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Выберите группу администрирования для Сервера администрирования.
3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания политики.
4. В открывшемся окне в списке выберите название приложения Kaspersky Endpoint Security для Linux.
5. Укажите **Стандартный режим или режим Агента Endpoint Detection and Response** приложения Kaspersky Endpoint Security для Linux.
6. Примите решение об использовании Kaspersky Security Network.
7. Ознакомьтесь с рекомендациями по оптимизации для управляемых устройств.
8. В названии политики укажите принадлежность политики к Серверу администрирования.
9. Отключите опцию **Наследовать параметры родительской политики**.
10. Сохраните внесенные изменения.

Видео: создание политики



5. Создание групповой задачи Обновление для Kaspersky Endpoint Security для Linux

1. В главном окне Web Console выберите раздел **Задачи**.
2. Выберите группу администрирования для Сервера администрирования.
3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задач.
4. В открывшемся окне в списке выберите название приложения Kaspersky Endpoint Security для Linux.
5. Укажите тип задачи *Обновление* и пройдите следующие шаги без изменения параметров.

   Запустится окно свойств задачи.
6. В разделе **Параметры приложения** → **Источники обновлений** включите источник Kaspersky Security Center и поднимите его приоритет.

В изолированных сетях используйте утилиту Kaspersky Update Utility для формирования хранилища для задач обновления.

Видео: настройка централизованного обновления баз



6. Добавление лицензионного ключа в хранилище Сервера администрирования с функцией автоматического распространения

1. В главном окне Kaspersky Security Center Web Console выберите раздел **Лицензии**.
2. Нажмите на кнопку **Добавить**.
3. Укажите опцию **Код активации** и нажмите **Отправить**.

   В изолированных сетях используйте файл ключа, который можно запросить с помощью сервиса https://keyfile.kaspersky.com/ru-RU.
4. В списке лицензий нажмите на название лицензии.
5. Установите флажок **Автоматически распространять лицензионный ключ на управляемые устройства**.
6. Сохраните изменения.

Видео: активация приложения с помощью кода активации



Видео: активация приложения с помощью файла ключа



7. Создание инсталляционных пакетов Агента администрирования и Kaspersky Endpoint Security для Linux

1. В главном окне Web Console выберите **Управление программным обеспечением → Инсталляционные пакеты**.
2. Нажмите на кнопку **Добавить**.

   Запустится Мастер создания инсталляционного пакета.
3. Выберите **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**.
4. В списке приложений найдите последнюю версию Kaspersky Endpoint Security для Linux и нажмите на название.
5. В боковой панели инициируйте загрузку кнопкой **Скачать и создать инсталляционный пакет**.

   Ознакомьтесь и примите лицензионные соглашения для начала использования приложений.
6. Вернитесь в список приложений и загрузите последнюю версию Агента администрирования (Kaspersky Network Agent for Linux).

   Ознакомьтесь и примите лицензионные соглашения для начала использования приложений.
7. В главном окне Web Console в списке загруженных приложений нажмите на названия приложений.

В изолированных сетях скачайте дистрибутивы с сайта "Лаборатории Касперского" и выберите в Мастере создания инсталляционного пакета опцию **Создать инсталляционный пакет из файла**.

Видео: создание инсталляционного пакета автоматически в Kaspersky Security Center



Видео: создание инсталляционного пакета вручную из файла в Kaspersky Security Center



8. Установка Агента администрирования для Linux

1. В главном окне Web Console выберите **Управление программным обеспечением → Инсталляционные пакеты**.
2. Установите флажок напротив пакета **Агента администрирования (Kaspersky Network Agent for Linux)**.
3. Нажмите **Развернуть**.

   Запустится Мастер развертывания защиты.
4. Выберите вариант **С использованием автономного инсталляционного пакета**.
5. На шаге **Перемещение устройств в папку Управляемые устройства** пропустите настройку правил перемещения устройств в группу администрирования. Эта опция не применяется для устройства Сервера администрирования.
6. На шаге **Результат формирования автономного инсталляционного пакета** выделите и скопируйте полный путь размещения скрипта установки приложения.
7. В операционной системе Сервера администрирования откройте командную строку.
8. Запустите установку автономного пакета:

   ```
   sudo bash "</var/opt/.../stand-alone_package_sh>"
   ```

   где `</var/opt/.../stand-alone_package_sh>` – это ранее скопированный полный путь к файлу скрипта автономного инсталляционного пакета приложения.

   В случае успешной установки отобразится соответствующее уведомление.
9. Переместите устройство Сервера администрирования (например, *ksclinux*) из группы **Управляемые устройства** в ранее подготовленную группу администрирования (например, *kscserver*).

9. Установка Kaspersky Endpoint Security для Linux

1. В главном окне Web Console выберите **Управление программным обеспечением → Инсталляционные пакеты**.
2. Установите флажок напротив пакета Kaspersky Endpoint Security для Linux.

3. Нажмите **Развернуть**.

   Запустится Мастер развертывания защиты.

4. Выберите вариант **С использованием автономного инсталляционного пакета**.

5. На шаге **Результат формирования автономного инсталляционного пакета** выделите и скопируйте полный путь размещения скрипта установки приложения.

6. В операционной системе Сервера администрирования откройте командную строку.

7. Запустите установку автономного пакета:

   ```
   sudo bash "</var/opt/.../stand-alone_package_sh>"
   ```

   где `</var/opt/.../stand-alone_package_sh>` – это ранее скопированный полный путь к файлу скрипта автономного инсталляционного пакета приложения.

   В случае успешной установки отобразится соответствующее уведомление.

8. В главном окне Web Console в разделе **Задачи** выберите корневой узел в списке групп администрирования с названием Сервера администрирования.

9. Из списка задач Сервера администрирования последовательно запустите следующие задачи:

   - Загрузка обновлений в хранилище Сервера администрирования.
   - Обновление (Kaspersky Endpoint Security для Linux).

10. В главном окне Web Console выберите **Управление активами** → **Управляемые устройства**.

11. Нажмите на имя объекта устройства Сервера администрирования.

12. Проверьте значения основных показателей состояния устройства:

    - Последнее обновление антивирусных баз (актуально).
    - Подключено к Серверу администрирования (актуально).
    - Состояние защиты (Выполняется).
    - Событие *Ключ успешно добавлен* (есть).

Используйте сценарий развертывания Kaspersky Endpoint Security для Linux для развертывания приложения на устройствах сети.

Перенос данных в Kaspersky Security Center с помощью мастера переноса данных

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

Перенос данных в Kaspersky Security Center возможен с Kaspersky Security Center Windows версии 15.1.0.28509 или выше.

Особенности переноса данных

- Частичное резервное копирование данных Сервера администрирования.
- Возможен выбор объектов для переноса.
- Группа администрирования или ее подгруппа, которую нужно перенести, может содержать не более 10 000 устройств.
- Используется для частичного переноса данных Сервера администрирования, включая только групповые объекты в пределах области переноса данных; групповые объекты вне области переноса данных необходимо восстановить вручную.

Область действия переноса данных

- Структура групп администрирования.
- Управляемые устройства, включенные в группы администрирования (не более 10 000 устройств).
- Теги, присвоенные перенесенным устройствам.
- Глобальные задачи Агента администрирования и управляемые приложения (не для Сервера администрирования).
- Групповые задачи Агента администрирования и управляемых приложений.
- Политики управляемых приложений.
- Шаблоны отчетов.
- Роли пользователей.
- Внутренние пользователи и группы безопасности.
- Пользовательские категории приложений, пополняемые вручную.
- Пользовательские выборки устройств.

Ограничения

- Перенос данных возможен только из Kaspersky Security Center Windows версии 15.1.0.28509 и выше в Kaspersky Security Center Linux версии 15 и выше.
- Вы можете выполнить этот сценарий только с помощью Kaspersky Security Center Web Console.
- Переносу не подлежат следующие области действия:
  - Глобальные задачи Сервера администрирования.
  - События, сохраненные на Сервере администрирования.
  - Хранилище дистрибутивов приложений для удаленной установки.

- Сертификат Сервера администрирования.
- Лицензионные ключи, используемые Сервером администрирования и управляемыми приложениями.
- Виртуальные Серверы администрирования.
- Параметры политики Агента администрирования.
- Правила перемещения устройств.
- Правила автоматического назначения тегов устройствам.
- Точки распространения.
- Параметры приложения "Лаборатории Касперского" сохраненные на Сервере администрирования.

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

- Функциональные различия Kaspersky Security Center Windows и Kaspersky Security Center Linux
- Список приложений "Лаборатории Касперского", поддерживаемых приложением Kaspersky Security Center Linux

Этапы

Сценарий переноса данных состоит из следующих этапов:

1 Предварительные действия

Этот шаг содержит инструкции по подготовке ранее настроенного Сервера администрирования для дальнейшей миграции на новый Сервер администрирования Kaspersky Security Center Linux. Подготовка состоит из следующих этапов:

1. Проверка версии Сервера администрирования для создания совместимой с Kaspersky Security Center Linux резервной копии.

   Все актуальные версии **Kaspersky Security Center Linux** поддерживают перенос данных с обновлением на более новую версию приложения. Создание и восстановление резервных копий возможно только в рамках одного типа СУБД.

   Для **Kaspersky Security Center Windows** необходимо проверить версию Сервера администрирования в **Свойства** → **Общие** → **Версия**. Если версия ниже, чем 15.1.0.28509, обновите Kaspersky Security Center Windows до последней версии.

   Обновление Kaspersky Security Center Windows до последней версии

   1. На сайте "Лаборатории Касперского" скачайте дистрибутив, соответствующий языку локализации установленного Сервера администрирования: `Version 15.1.0.28509 | Windows | Full distributive`.

      Исполняемый файл сохраняется в папку **Загрузки** со следующим названием: `ksc_15.1_<build number>_full_<language>.exe`.

2. Скопируйте дистрибутив на Сервер администрирования.

3. Запустите от администратора исполняемый файл `ksc_15.1_<build number>_full_<language>.exe`.

4. В открывшемся окне нажмите на ссылку **Установить Kaspersky Security Center**.

   Запустится мастер установки Сервера администрирования.

5. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения следующих документов** установите флажки:

   - **Условия и положения настоящего Лицензионного соглашения**.
   - **Политику конфиденциальности, которая описывает обработку данных**.

6. Выберите **Обновить Сервер администрирования и консоль на основе веб-интерфейса (рекомендуется)** и перейдите к следующему шагу.

7. Создайте новую резервную копию, выберите опцию **Я хочу создать резервную копию данных** и пройдите мастер создания резервной копии.

8. Нажмите **Обновить**.

9. Во время обновления в мастере установки Web Console подтвердите все шаги мастера для обновления версии.

   Процесс установки обновления Сервера администрирования займет некоторые время. После завершения мастера установки Консоль администрирования может не принимать подключения до завершения инициализации базы данных.

10. Дождитесь полного завершения процедуры обновления.

2. Проверка выполнения требований к сертификату Сервера администрирования.

   Перед созданием резервной копии вам нужно убедиться, что сертификат содержит альтернативное имя субъекта (Subject Alternative Name, SAN). Если нет, важно заменить сертификат, иначе вы не сможете войти в Web Console после восстановления из резервной копии.

   Чтобы проверить, что сертификат включает альтернативное имя субъекта:

   - Для устройств с операционной системой Windows:

     a. В Консоли администрирования выберите Сервер администрирования, для которого требуется проверка.

     b. В контекстном меню выберите пункт **Свойства** → **Общие** → **Просмотреть сертификат Сервера**.

     c. В открывшемся окне проверьте значение пункта **Альтернативное имя субъекта**.

   - Для устройств с операционной системой Linux выполните команду:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   Убедитесь, что альтернативное имя субъекта содержит доменное имя (DNS) устройства Сервера администрирования.

Если значение содержит только внешний IP-адрес без доменного имени (DNS) или значение полностью отсутствует, вручную замените сертификат на соответствующий требованиям работы с Kaspersky Security Center Linux. Замените общий сертификат Сервера администрирования с помощью утилиты klsetsrvcert.

Замена общего сертификата Сервера администрирования с помощью утилиты klsetsrvcert

1. Создайте новый сертификат с отложенной датой начала использования на устройствах, выполнив команду:

   - Для Kaspersky Security Center Windows:

     ```
     "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -t CR -g "
     <oldksc.example.internal>" -o "RsaKeyLen:2048"
     ```

   - Для Kaspersky Security Center Linux:

     ```
     /opt/kaspersky/ksc64/sbin/klsetsrvcert -t CR -g "<oldksc.example.internal>" -o "RsaKeyLen:2048"
     ```

   где `"<oldksc.example.internal>"` – FQDN-адрес подключения к Серверу администрирования.

   > Не используйте IP-адрес для этого значения.

2. Назначьте дату начала использования нового сертификата на всех устройствах, выполнив команду:

   - Для Kaspersky Security Center Windows:

     ```
     "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -f "DD-MM-YYYY hh:mm"
     ```

   - Для Kaspersky Security Center Linux:

     ```
     /opt/kaspersky/ksc64/sbin/klsetsrvcert -f "DD-MM-YYYY hh:mm"
     ```

   где дата `"DD-MM-YYYY hh:mm"` минимум на 30 дней больше текущей. По умолчанию период распространения нового сертификата (`CR`) составляет 90 дней.

   > После наступления назначенного времени может потребоваться переустановить Web Console чтобы восстановить к ней доступ и актуализировать сертификат в ее составе.

3. Если необходимо, после миграции на новый Сервер администрирования запустите утилиту klmover, чтобы восстановить соединение устройств с Сервером администрирования. Запуск утилиты может понадобиться, если устройство было выключено весь период распространения сертификата или не подключалось к Серверу администрирования.

2 Выберите способ переноса данных

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

- Перенос данных с использованием иерархии Серверов администрирования

  Выберите этот параметр, если Сервер администрирования Kaspersky Security Center Windows является подчиненным по отношению к Серверу администрирования Kaspersky Security Center Linux. Вы управляете процессом переноса данных и переключаетесь между Серверами в рамках одного экземпляра Kaspersky Security Center Web Console. Если вы предпочитаете этот вариант, вы можете организовать Серверы администрирования в иерархию, чтобы упростить процедуру переноса данных. Для этого создайте иерархию перед началом переноса данных.

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

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

3 Создание резервной копии сертификата и закрытого ключа Сервера администрирования Kaspersky Security Center Windows (необязательный шаг)

Возможно, вы захотите поместить управляемые устройства под управление Сервера администрирования Kaspersky Security Center Linux, восстановив сертификат и закрытый ключ Сервера администрирования из резервной копии. В этом случае создайте резервную копию сертификата и закрытого ключа Сервера администрирования Kaspersky Security Center Windows. Затем на шаге 7 вам необходимо восстановить сертификат и закрытый ключ.

4 Экспорт данных из Kaspersky Security Center Windows

Откройте Kaspersky Security Center Windows и запустите мастер переноса данных.

5 Импорт данных в приложение Kaspersky Security Center Linux

Продолжите работу мастера переноса данных, чтобы импортировать экспортированные данные в Kaspersky Security Center Linux. Если Серверы организованы в иерархию, импорт начинается автоматически после успешного экспорта в том же мастере. Если Серверы не выстроены в иерархию, вы продолжите работу мастера переноса данных после перехода на Kaspersky Security Center Linux.

6 Выполнение дополнительных действий для переноса объектов и параметров из Kaspersky Security Center Windows в Kaspersky Security Center Linux вручную (необязательный шаг)

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

- Перенести лицензионные ключи, используемые Сервером администрирования и управляемыми приложениями.
- Настроить глобальные задачи Сервера администрирования.
- Настроить параметры политики Агента администрирования.
- Создать инсталляционные пакеты приложений.
- Создать виртуальные Серверы администрирования.
- Создать правила перемещения устройств.
- Настроить правила автоматического назначения тегов устройствам.
- Создать категории приложений.
- Назначить и настроить точки распространения.

  Если вы перемещаете устройство, которое действует как точка распространения, на другой Сервер администрирования, устройства, включенные в область действия точки распространения, не перемещаются автоматически. Вам нужно переместить каждое устройство по отдельности. Если точка распространения выполняет роль шлюза соединения, вам нужно запустить скрипт `# /opt/kaspersky/klnagent64/bin/setup/postinstall.pl`, чтобы точка распространения больше не выполняла роль шлюза соединения.

7 Переместить импортированные управляемые устройства под управление Kaspersky Security Center Linux

Завершите перенос данных, переместите импортированные управляемые устройства под управление Kaspersky Security Center Linux. Вы можете воспользоваться одним из следующих способов:

- С помощью утилиты klmover.

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

- С помощью задачи *Смена сервера администрирования*.

  Создайте задачу *Сменить Сервер администрирования*, укажите импортированные управляемые устройства, новый Сервер администрирования и другие параметры задачи. Затем запустите задачу, чтобы поместить управляемые устройства под управление Сервера администрирования Kaspersky Security Center Linux.

- С помощью удаления (если уже установлен) и дальнейшей установки Агента администрирования на управляемых устройствах.

  Создайте инсталляционный пакет Агента администрирования и укажите параметры подключения для нового Сервера администрирования в свойствах инсталляционного пакета. Удалите Агент администрирования на импортированных управляемых устройствах, а затем используйте инсталляционный пакет для установки Агента администрирования на этих устройствах с помощью задачи удаленной установки. Вы также можете создать и использовать автономный инсталляционный пакет для локальной установки Агента администрирования. Подробнее см. в разделе Переключение управляемых устройств под управление Kaspersky Security Center Linux.

- С помощью восстановления сертификата и закрытого ключа Сервера администрирования из резервной копии (только для переноса данных в Kaspersky Security Center Linux версии 15.1 и выше).

  Назначьте устройству с Сервером администрирования Kaspersky Security Center Linux тот же сетевой адрес, что и у устройства с Сервером администрирования Kaspersky Security Center Windows. Запустите утилиту klbackup с параметром `-cert_only`, чтобы восстановить сертификат Сервера администрирования и закрытый ключ из резервной копии, сохраненной на шаге 3. Выполните следующую команду в командной строке: `/opt/kaspersky/ksc64/sbin/klbackup -path <путь к резервной копии сертификата Сервера администрирования> -restore -cert_only`.

8 Обновите Агент администрирования до последней версии.

Обновите Агент администрирования для Linux до той же версии, что и Kaspersky Security Center.

9 Убедитесь, что управляемые устройства отображаются на новом Сервере администрирования.

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

Другие способы переноса данных

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

- Экспортируйте задачи из Kaspersky Security Center Windows, а затем импортируйте задачи в Kaspersky Security Center Linux.

- Экспортируйте определенные политики из Kaspersky Security Center Windows, а затем импортируйте политики в Kaspersky Security Center Linux. Связанные профили политик экспортируются и импортируются вместе с выбранными политиками.

Экспорт групповых объектов из Kaspersky Security Center Windows

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

Вы можете экспортировать следующие объекты:

- Задачи и политики управляемых приложений.
- Глобальные задачи.
- Пользовательские выборки устройств.
- Структуру групп администрирования и входящие в нее устройства.
- Теги, назначенные устройствам, данные которых вы переносите.

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

Чтобы экспортировать управляемые устройства и связанные групповые объекты с помощью мастера переноса данных:

1. В зависимости от того, организованы ли в иерархию Серверы администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux, выполните одно из следующих действий:
   - Если Серверы выстроены в иерархию, откройте Kaspersky Security Center Web Console и переключитесь на Сервер администрирования Kaspersky Security Center Windows.
   - Если Серверы не организованы в иерархию, откройте Kaspersky Security Center Web Console, подключенную к Kaspersky Security Center Windows.
2. В главном окне приложения перейдите в раздел **Операции** → **Перенос данных**.
3. Выберите **Перенос данных в Kaspersky Security Center Linux или Open Single Management Platform**, чтобы запустить мастер, и следуйте его шагам.
4. Выберите группу или подгруппу администрирования, которую вы хотите экспортировать. Обратите внимание, что в выбранной группе или подгруппе администрирования должно быть не более 10 000 устройств.

5. Выберите управляемые приложения, задачи и политики которых будут экспортированы. Выберите только те приложения, которые поддерживаются Kaspersky Security Center Linux. Объекты неподдерживаемых приложений все равно будут экспортированы, но не будут работать.

6. Используйте ссылки слева, чтобы выбрать глобальные задачи, выбранные устройства и отчеты для экспорта. Ссылка **Группировать объекты** позволяет исключить из экспорта роли пользователей, внутренних пользователей и группы безопасности, а также пользовательские категории приложений.

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

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

- Если Серверы не организованы в иерархию, файл экспорта загружается на ваше устройство.

При переносе данных с поддержкой иерархии Сервера администрирования импорт начинается автоматически после успешного экспорта. При переносе данных без поддержки иерархии Сервера администрирования вы можете вручную импортировать сохраненный файл экспорта в Kaspersky Security Center Linux.

Импорт файла экспорта в Kaspersky Security Center Linux

Чтобы передать информацию об управляемых устройствах, объектах и их параметрах, которые вы экспортировали из Kaspersky Security Center Windows, вам нужно импортировать ее в приложение Kaspersky Security Center Linux или Kaspersky Symphony XDR.

Чтобы импортировать управляемые устройства и связанные групповые объекты с помощью мастера переноса данных:

1. В зависимости от того, организованы ли в иерархию Серверы администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux, выполните одно из следующих действий:

   - Если Серверы организованы в иерархию, переходите к следующему шагу мастера переноса данных после завершения экспорта. Импорт начнется автоматически после успешного экспорта в этом мастере (см. шаг 2 этой инструкции).

   - Если Серверы не организованы в иерархию:

     a. Откройте приложение Kaspersky Security Center Web Console, подключенное к Kaspersky Security Center Linux или к Kaspersky Symphony XDR.

     b. В главном окне приложения перейдите в раздел **Операции** → **Перенос данных**.

     c. Выберите файл экспорта (ZIP-архив), который вы создали и загрузили при экспорте из Kaspersky Security Center Windows. Начнется загрузка файла экспорта.

2. После успешной загрузки файла экспорта вы можете продолжить импорт. Если вы хотите указать другой файл для экспорта, перейдите по ссылке **Изменить** и выберите нужный файл.

3. Отобразится вся иерархия групп администрирования Kaspersky Security Center Linux.

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

4. Начнется импорт объектов группы. Свернуть мастер переноса данных и выполнять любые параллельные операции во время импорта невозможно. Дождитесь, пока значки (🔄) рядом со всеми пунктами в списке объектов заменятся на зеленые флажки (✓) и импорт завершится.

5. Когда импорт завершится, экспортированная структура групп администрирования, включая сведения об устройствах, появится в целевой группе администрирования, которую вы выбрали. Если имя восстанавливаемого объекта совпадает с именем существующего объекта, к восстановленному будет добавлен дополнительный суффикс.

> Если в перенесенной задаче указаны данные учетной записи, под которой она запускается, вам нужно открыть задачу и ввести пароль еще раз после завершения импорта.

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

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

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

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

Для завершения переноса данных вам необходимо переключить управляемые устройства под управление Kaspersky Security Center Linux.

Переключение управляемых устройств под управление Kaspersky Security Center Linux

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

Вы можете переместить управляемые устройства под управление Kaspersky Security Center Linux одним из следующих способов:

- Используя утилиту klmover.
- Используя задачу *Смена Сервера администрирования*.

- Восстановив сертификат и закрытый ключ Сервера администрирования из резервной копии (только для переноса данных в Kaspersky Security Center Linux 15.1 и выше).

  Подробнее см. шаг "Переместить импортированные управляемые устройства под управление Kaspersky Security Center Linux" основного сценария переноса данных.

- Установив Агент администрирования на управляемые устройства с помощью задачи удаленной установки.

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

1. Удалите Агент администрирования на импортированных управляемых устройствах, которые будут переключены под управление Kaspersky Security Center Linux.

2. Переключитесь на Сервер администрирования Kaspersky Security Center Windows.

3. Перейдите в раздел **Управление программным обеспечением → Инсталляционные пакеты** и откройте свойства существующего инсталляционного пакета Агента администрирования.

   Если инсталляционный пакет Агента администрирования отсутствует в списке пакетов, загрузите новый.

   Вы также можете создать и использовать автономный инсталляционный пакет для локальной установки Агента администрирования.

4. На вкладке **Параметры** выберите раздел **Подключение**. Укажите параметры подключения Сервера администрирования Kaspersky Security Center Linux.

5. Создайте задачу удаленной установки для импортированных управляемых устройств, а затем укажите перенастроенный инсталляционный пакет Агента администрирования.

   Вы можете установить Агент администрирования с помощью Сервера администрирования Kaspersky Security Center Windows или с помощью устройства под управлением Windows, которое выполняет роль точки распространения. Если вы используете Сервер администрирования, включите параметр **Средствами операционной системы с помощью Сервера администрирования**. Если вы используете точку распространения, включите параметр **Средствами операционной системы с помощью точек распространения**.

6. Запустите задачу удаленной установки приложения.

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

Настройка Сервера администрирования

В этом разделе описан процесс настройки и свойства Сервера администрирования.

Настройка адреса подключения Сервера администрирования

Адрес подключения к Серверу администрирования – это сетевой адрес, который используется для следующих целей:

- Как адрес по умолчанию при создании инсталляционных пакетов Агента администрирования.

  После установки Агента администрирования управляемые устройства подключаются к Серверу администрирования по этому адресу.

- Как адрес прокси-сервера KSN.

  Управляемые устройства подключаются к прокси-серверу KSN с по этому адресу.

Чтобы настроить адрес подключения Сервера администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Общие**.

3. В открывшемся окне в поле **Адрес подключения Сервера администрирования** укажите новый адрес подключения Сервера администрирования.

   Максимальная длина адреса подключения составляет 255 символов.

   Вы можете указать адрес подключения к Серверу администрирования как NetBIOS-имя, FQDN или IP-адрес Сервера администрирования.

4. Нажмите на кнопку **Сохранить**.

Указанный адрес используется в качестве адреса Сервера администрирования и адреса прокси-сервера KSN.

Настройка параметров подключения Kaspersky Security Center Web Console к Серверу администрирования

Вы можете настроить подключение Kaspersky Security Center Web Console к Серверу администрирования через свойства Сервера администрирования или с помощью параметров политики Сервера администрирования.

Чтобы задать порты подключения с помощью свойств Сервера администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

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

3. При необходимости укажите **SSL-порт для Kaspersky Security Center Web Console** или укажите другие порты подключения к Серверу администрирования.

Основные параметры подключения выбранного Сервера указаны.

Чтобы задать порты подключения с помощью свойств политики Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами → Политики**.

2. Нажмите на название политики Сервера администрирования и перейдите на вкладку **Параметры приложения**.

3. При необходимости укажите **SSL-порт для Kaspersky Security Center Web Console** или укажите другие порты подключения к Серверу администрирования.

   Если вы выключите параметр **Открыть порт для Kaspersky Security Center Web Console** и этот параметр политики будет применен к устройству, вы не сможете подключиться к Серверу администрирования с помощью Kaspersky Security Center Web Console. В этом случае соединение будет прервано. Если у вас есть Сервер администрирования, на котором не применяется эта политика, вы можете повторно подключиться к этому Серверу администрирования с помощью Kaspersky Security Center Web Console.

Основные параметры подключения выбранного Сервера указаны.

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

По умолчанию подключения к Kaspersky Security Center Linux разрешены с любого устройства. Например, вы можете установить Сервер Kaspersky Security Center Web Console на любое устройство, которое соответствует требованиям, и Сервер Kaspersky Security Center Web Console будет взаимодействовать с Kaspersky Security Center Linux. 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 Linux через Сервер Kaspersky Security Center Web Console, установленный на устройстве, которое не включено в список разрешенных, они не смогут войти в Kaspersky Security Center Linux.

IP-адрес проверяется, когда пользователь входит в Kaspersky Security Center Linux или запускает приложение, которое взаимодействует с Сервером администрирования через Kaspersky Security Center Linux OpenAPI. В этот момент приложение 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 приложений:

- Сервер Kaspersky Security Center Web Console.

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

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

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

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

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

Как создать список разрешенных IP-адресов

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

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

1. На устройстве Сервера администрирования запустите командную строку под учетной записью с правами администратора.

2. Измените текущую папку на папку установки Kaspersky Security Center Linux (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 параметров доступа Сервера администрирования к интернету

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

Чтобы указать параметры доступа Сервера администрирования к интернету:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры доступа к сети интернет**.

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

   Адрес прокси-сервера

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.

Также можно настроить доступ в интернет с помощью мастера первоначальной настройки.

Иерархия Серверов администрирования

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

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

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

Главный Сервер администрирования получает данные только от невиртуальных подчиненных Серверов администрирования в рамках перечисленных выше параметров. Это ограничение не распространяется на виртуальные Серверы администрирования, которые совместно используют базу данных со своим главным Сервером администрирования.

Иерархия Серверов администрирования поддерживает мультитенантный режим. Этот режим позволяет Главному администратору централизованно управлять независимо несколькими клиентами. Каждая организация-клиент или офис изолированы от других и называются тенантами. Вы можете выделить несколько управляемых устройств вместе со связанными с ними данными, параметрами, политиками и задачами для тенанта, а также настроить права пользователей для каждого тенанта.

Главный Сервер администрирования, установленный в основной инфраструктуре организации, выполняет в роль главного тенанта. Главный Сервер администрирования позволяет подчиненным или виртуальным Серверам администрирования (и его изолированным тенантам) независимо получать и обрабатывать свои события, а также работать со своими ресурсами, службами и конфигурациями.

Поставщик услуг, у которого есть несколько организаций-клиентов, может предоставить функциональность Kaspersky Security Center Linux, включая агрегирование алертов и действия по реагированию, каждой организации-клиенту независимо. Для этого поставщик услуг подключает подчиненные или виртуальные Серверы администрирования в качестве тенантов для каждой организации-клиента. Поставщик услуг предоставляет услуги, используя свой собственный персонал и ресурсы.

Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования

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

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

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

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

1. Убедитесь, что на будущем главном Сервере администрирования доступен порт 13000.

   Этот порт будет использоваться для взаимодействия между главным Сервером администрирования и подчиненным Сервером администрирования после построения иерархии.

2. Перейдите в свойства будущего главного Сервера администрирования:

   a. В главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**.

   b. В открывшейся панели наведите курсор мыши на название нужного Сервера администрирования и нажмите на значок параметров (⚙).

      Вы также можете нажать на имя Сервера администрирования, а после того как имя отобразится в главном меню, нажать на него в главном меню, чтобы открыть окно свойств Сервера.

3. В открывшемся окне свойств перейдите на вкладку **Серверы администрирования**.

4. Установите флажок рядом с именем группы администрирования, в которую вы хотите добавить Сервер администрирования.

5. В меню выберите пункт **Подключить подчиненный Сервер администрирования**.

   Запустится мастер добавления подчиненного Сервера администрирования. Для продолжения работы мастера нажмите на кнопку **Далее**.

6. Заполните следующие поля:

   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.

   Отображаемое имя подчиненного Сервера

   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

   Укажите IP-адрес или доменное имя подчиненного Сервера администрирования.

   Этот параметр необходим, если включен параметр **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.

   Номер SSL-порта Сервера

   После построения иерархии укажите номер SSL-порта, который будет использоваться для взаимодействия между главным Сервером администрирования и подчиненным Сервером администрирования. По умолчанию установлен порт 13000.

   API-порт Сервера

   Номер порта, который Web Console будет использовать для приема подключений от подчиненного Сервера администрирования по OpenAPI. По умолчанию установлен порт 13299.

   При построении иерархии Web Console подключается к будущему подчиненному Серверу, запрашивает учетные данные, получает открытый сертификат и выполняет первоначальную настройку.

   После построения иерархии Сервера администрирования порт 13299 больше не будет использоваться. Серверы администрирования будут взаимодействовать через порт 13000.

   Сертификат подчиненного Сервера администрирования

Добавьте файл сертификата. Можно либо вручную загрузить сертификат с вашего устройства, либо получить сертификат с подчиненного Сервера администрирования.

7. Укажите параметры подключения и аутентификации.

   - Введите адрес будущего главного Сервера администрирования.
   - Выберите параметр **Использовать прокси-сервер**, если вы используете прокси-сервер для подключения подчиненного Сервера администрирования.

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

     - **Адрес прокси-сервера**
     - **Имя пользователя**
     - **Пароль**

8. Введите учетные данные пользователя, имеющего права доступа на будущий подчиненный Сервер администрирования.

Работа мастера завершена, будущий подчиненный Сервер подключен и иерархия "главный/подчиненный" построена.

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.

Подключиться не удается в следующих случаях:

- Неправильные параметры подключения.

  Вам нужно проверить параметры или указать сертификат будущего подчиненного Сервера вручную.

- Будущий подчиненный Сервер выполняет аутентификацию с помощью самоподписанного сертификата, автоматически сгенерированного Kaspersky Security Center Linux. В результате браузер может заблокировать загрузку самоподписанного сертификата.

  Вы можете выполнить одно из следующих действий:

  - Для будущего подчиненного Сервера создать сертификат, доверенный в вашей инфраструктуре и соответствующий требованиям к пользовательским сертификатам.
  - Добавить самоподписанный сертификат будущего подчиненного Сервера в список доверенных сертификатов браузера. Рекомендуется использовать этот параметр только в том случае, если вы не можете создать пользовательский сертификат. Информацию о добавлении сертификата в список доверенных сертификатов см. в документации вашего браузера.

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

Если вы не можете подключится к будущему подчиненному Серверу администрирования (например, потому что он был временно отключен, недоступен или потому что файл сертификата подчиненного Сервера администрирования является самоподписанным), вы все равно можете добавить подчиненный Сервер администрирования.

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

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

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

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

   a. Нажмите на имя Сервера администрирования.

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

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

   d. Выберите тип главного Сервера администрирования.

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

   f. Выберите ранее сохраненный файл сертификата будущего главного Сервера, нажав **Укажите сертификат главного Сервера администрирования**.

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

   h. Если подключение к будущему главному Серверу администрирования выполняется с помощью прокси-сервера, выберите параметр **Использовать прокси-сервер** и задайте параметры подключения.

   i. 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:

1. В главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**).
2. В верхней части страницы нажмите на кнопку **Показать иерархию**.

   В открывшейся панели навигации отобразится список подчиненных (в том числе виртуальных) Серверов администрирования. Вы можете перейти на любой из этих Серверов администрирования, нажав на его имя.

Вы не сможете перейти к виртуальным Серверам администрирования, если вы открыли панель навигации из разделов **IP-диапазоны** и **Удаленные объекты**.
Также отображаются группы администрирования. Группы доступны для управления, если вы открыли панель навигации из следующих разделов: **Управляемые устройства**, **Политики**, **Задачи** и **Точки распространения**. Иначе группы отображаются серым цветом.

Если вы подключены к главному Серверу администрирования в Kaspersky Security Center Web Console и не можете подключиться к виртуальному Серверу администрирования, управляемому подчиненным Сервером администрирования, вы можете воспользоваться одним из следующих способов:

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

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

     Запустится мастер установки приложения. 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 приложения нажмите на кнопку **Готово**.

- Используйте Kaspersky Security Center 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 Web Console.

Управление виртуальными Серверами администрирования

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

- создание виртуальных Серверов администрирования;
- включение и выключение виртуальных Серверов администрирования;
- назначение администратора виртуального Сервера администрирования;
- смена Сервера администрирования для клиентских устройств;
- удаление виртуальных Серверов администрирования.

Создание виртуального Сервера администрирования

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

При создании виртуального Сервера администрирования он наследует список пользователей и все права пользователей главного Сервера администрирования. Если пользователь имеет права доступа к главному Серверу, этот пользователь также имеет права доступа к виртуальному Серверу. После создания вы самостоятельно настраиваете права доступа к Серверам.

Чтобы создать и добавить виртуальный Сервер администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.
2. На открывшейся странице перейдите на вкладку **Серверы администрирования**.
3. Выберите группу администрирования, в которую вы хотите добавить виртуальный Сервер администрирования.
   Виртуальный Сервер администрирования будет управлять устройствами из выбранной группы (включая подгруппы).
4. В меню выберите пункт **Новый виртуальный Сервер администрирования**.
5. На открывшейся странице задайте свойства нового виртуального Сервера администрирования:
   - **Имя виртуального Сервера администрирования**.
   - **Адрес подключения Сервера администрирования**.
     Вы можете указать имя или IP-адрес Сервера администрирования.

6. Из списка пользователей выберите администратора виртуального Сервера администрирования. Существующую учетную запись при необходимости можно изменить перед тем, как назначить ей роль администратора; можно также создать новую учетную запись.

   При необходимости вы можете создать учетную запись, которая будет выполнять роль администратора виртуального Сервера администрирования с помощью утилиты kladduser. Для этого используйте следующую команду:

   ```
   kladduser -n <user_name> -p <password> -vs <virtual_server_name>
   ```

   Где virtual_server_name – имя виртуального Сервера администрирования.

7. Нажмите на кнопку **Сохранить**.

Новый виртуальный Сервер администрирования создан, добавлен в группу администрирования и отображается на вкладке **Серверы администрирования**.

Если вы подключены к главному Серверу администрирования в Kaspersky Security Center Web Console и не можете подключиться к виртуальному Серверу администрирования, управляемому подчиненным Сервером администрирования, вы можете воспользоваться одним из следующих способов:

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

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

     Запустится мастер установки приложения. 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 приложения нажмите на кнопку **Готово**.

- Используйте Kaspersky Security Center 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 Web Console.

Включение и выключение виртуального Сервера администрирования

Когда вы создаете виртуальный Сервер администрирования, он по умолчанию включается. Вы можете выключить или снова включить его в любое время. Выключение или включение виртуального Сервера администрирования равносильно выключению или включению физического Сервера администрирования.

Чтобы включить или выключить виртуальный Сервер администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.
2. На открывшейся странице перейдите на вкладку **Серверы администрирования**.
3. Выберите виртуальный Сервер администрирования, который вы хотите включить или выключить.
4. В меню нажмите на кнопку **Подключить / отключить виртуальный Сервер администрирования**.

Состояние виртуального Сервера администрирования изменяется на включено или выключено в зависимости от его предыдущего состояния. Обновленное состояние отображается рядом с именем Сервера администрирования.

Назначение администратора виртуального Сервера администрирования

Если вы используете в своей организации виртуальные Серверы администрирования, вам может потребоваться назначить отдельного администратора для каждого виртуального Сервера администрирования. Например, это может быть полезно, когда вы создаете виртуальные Серверы администрирования для управления отдельными офисами или отделами вашей организации или если вы являетесь поставщиком услуг (MSP) и управляете своими тенантами с помощью виртуальных Серверов администрирования.

При создании виртуального Сервера администрирования он наследует список пользователей и все права пользователей главного Сервера администрирования. Если пользователь имеет права доступа к главному Серверу, этот пользователь также имеет права доступа к виртуальному Серверу. После создания вы самостоятельно настраиваете права доступа к Серверам. Если вы хотите назначить администратора только для виртуального Сервера администрирования, убедитесь, что у администратора нет прав доступа на главном Сервере администрирования.

Вы назначаете администратора виртуального Сервера администрирования, предоставляя права доступа администратору к виртуальному Серверу администрирования. Вы можете предоставить требуемые права доступа одним из следующих способов:

- Настройте права доступа для администратора вручную.
- Назначьте одну или несколько пользовательских ролей администратору.

Чтобы войти в Kaspersky Security Center Web Console, администратор виртуального Сервера администрирования указывает имя виртуального Сервера администрирования, имя пользователя и пароль. Kaspersky Security Center Web Console выполняет аутентификацию администратора и открывает виртуальный Сервер администрирования, к которому у администратора есть права доступа. Администратор не может переключаться между Серверами администрирования.

Предварительные требования

Убедитесь, что выполнены следующие условия:

- Виртуальный Сервер администрирования создан.
- На главном Сервере администрирования у вас создана учетная запись для администратора, которого вы хотите назначить для виртуального Сервера администрирования.
- У вас есть право **Изменение списков управления доступом объектов** в функциональной области **Общие функции → Права пользователей**.

Настройка прав доступа вручную

Чтобы назначить администратора виртуального Сервера администрирования:

1. Переключитесь на нужный виртуальный Сервер администрирования:
   a. В главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**.
   b. В открывшейся панели нажмите на имя нужного виртуального Сервера администрирования.

   > Вы не можете переключиться на виртуальный Сервер администрирования из разделов **IP-диапазоны** и **Удаленные объекты**.

   В главном меню Сервер администрирования изменится на тот, который вы выбрали.
2. Перейдите в свойства Сервера администрирования, нажав на его имя в главном меню.

   Или в панели наведите курсор мыши на название нужного виртуального Сервера администрирования и нажмите на значок параметров (⚙).

   Откроется окно свойств Сервера администрирования.
3. На вкладке **Права доступа** нажмите на кнопку **Добавить**.

   Откроется единый список пользователей главного Сервера администрирования и текущего виртуального Сервера администрирования.
4. В списке пользователей выберите учетную запись администратора, которого вы хотите назначить для виртуального Сервера администрирования, и нажмите на кнопку **OK**.

   Приложение добавляет выбранного пользователя в список пользователей на вкладку **Права доступа**.
5. Установите флажок рядом с добавленной учетной записью и нажмите на кнопку **Права доступа**.
6. Настройте права администратора на виртуальном Сервере администрирования.

Для успешной аутентификации администратор должен иметь следующие права:

- право **Чтение** в функциональной области **Общие функции → Базовая функциональность**.
- право **Чтение** в функциональной области **Общие функции → Виртуальные Серверы администрирования**.

Приложение сохраняет измененные права пользователя в учетной записи администратора.

Чтобы назначить администратора нескольким виртуальным Серверам администрирования:

1. В главном окне приложения нажмите на имя главного Сервера администрирования.
2. На открывшейся странице перейдите на вкладку **Права доступа** и нажмите **Назначить**.

   В открывшемся окне **Добавить пользователей или группы** установите флажок рядом с пользователем, которого вы хотите назначить администратором.
3. Вы можете перейти на вкладку **Группы**, чтобы выбрать группы пользователей.
4. Нажмите на кнопку **Далее**.
5. Выберите серверы, для которых вы хотите назначить администратора, и нажмите **Далее**.
6. Выберите роли администратора, которые вы хотите назначить пользователю, если это необходимо.

   Если вы хотите установить пользовательские роли для текущего Сервера администрирования, перейдите в свойства нужного Сервера администрирования, нажмите **Назначить роли** и выберите пользовательские роли.
7. Нажмите на кнопку **Готово**, чтобы сохранить изменения.

Администратор с выбранными ролями теперь назначен нескольким виртуальным Серверам администрирования.

Чтобы отозвать права доступа администратора:

1. Переключитесь на нужный Сервер администрирования.
2. В главном окне приложения нажмите на имя Сервера администрирования.
3. На открывшейся странице перейдите на вкладку **Права доступа**.
4. Установите флажок рядом с пользователем, у которого вы хотите отозвать права доступа.
5. Нажмите **Отозвать** и подтвердите действие.

Права доступа выбранного пользователя отозваны.

Настройка прав доступа с помощью назначения пользовательских ролей

Также вы можете предоставить права доступа администратору виртуального Сервера администрирования через пользовательскую роль. Например, это может быть полезно, если вы хотите назначить несколько администраторов на один и тот же виртуальный Сервер администрирования. В этом случае вы можете назначить учетным записям администраторов одну или несколько пользовательских ролей вместо того, чтобы настраивать одни и те же права для нескольких администраторов.

Чтобы назначить администратора виртуального Сервера администрирования, назначив ему пользовательские роли:

1. На главном Сервере администрирования создайте пользовательскую роль и укажите все необходимые права доступа, которыми должен обладать администратор на виртуальном Сервере администрирования. Вы можете создать несколько ролей, например, если хотите разделить доступ к разным функциональным областям.

2. Переключитесь на нужный виртуальный Сервер администрирования:

   a. В главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**.

   b. В открывшейся панели нажмите на имя нужного виртуального Сервера администрирования.

   > Вы не можете переключиться на виртуальный Сервер администрирования из разделов **IP-диапазоны** и **Удаленные объекты**.

   В главном меню Сервер администрирования изменится на тот, который вы выбрали.

3. Назначьте новую роль или несколько ролей учетной записи администратора.

   Приложение назначает роль учетной записи администратора.

Настройка прав доступа на уровне объекта

В дополнение к назначению прав доступа на уровне функциональной области, вы можете настроить доступ к определенным объектам на виртуальном Сервере администрирования, например, к определенной группе администрирования или задаче. Для этого переключитесь на виртуальный Сервер администрирования, а затем настройте права доступа в свойствах объекта.

Смена Сервера администрирования для клиентских устройств

Вы можете сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером с помощью задачи *Смена Сервера администрирования*. После завершения задачи выбранные клиентские устройства будут под управлением указанного Сервера администрирования.

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

Чтобы сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. На шаге мастера **Параметры новой задачи** укажите следующие параметры:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Security Center**.

   b. В поле **Тип задачи** выберите **Смена Сервера администрирования**.

   c. В поле **Название задачи** укажите название создаваемой задачи.

   Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

   d. Выберите устройства, которым будет назначена задача:

   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 определенное приложение 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.

4. На шаге мастера **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

5. На этом шаге мастера подтвердите свое согласие с условиями смены Сервера администрирования для клиентских устройств.

6. На этом шаге мастера выберите Сервер администрирования, который вы хотите использовать для управления выбранными устройствами:

   Смена главного Сервера администрирования

   Чтобы переместить клиентские устройства на другой главный Сервер администрирования, укажите следующие параметры подключения к Серверу администрирования:

   1. В поле **Адрес Сервера администрирования** укажите адрес нового главного Сервера администрирования.

   2. В поле **Номер порта** укажите номер порта для подключения к Серверу администрирования.

      По умолчанию установлен порт 14000.

   3. В поле **SSL-порт** укажите номер SSL-порта главного Сервера администрирования.

      По умолчанию установлен порт 13000.

   4. При необходимости включите параметр **Использовать прокси-сервер**.

      Если этот параметр выключен, для подключения устройства к Серверу администрирования используется прямое соединение.

      Если этот параметр включен, укажите параметры прокси-сервера:

      - **Адрес прокси-сервера**

      - **Порт прокси-сервера**

      Если ваш прокси-сервер требует аутентификации, в полях **Имя пользователя** и **Пароль** укажите учетные данные учетной записи, под которой устанавливается соединение с прокси-сервером. Рекомендуется указывать данные учетной записи с минимальными правами, необходимыми только для аутентификации на прокси-сервере.

   5. При необходимости загрузите новый сертификат Сервера администрирования.

   Смена виртуального Сервера на этом главном Сервере

   Выберите этот параметр, чтобы переместить на виртуальный Сервер администрирования клиентские устройства на текущем главном Сервере администрирования. Для этого в раскрывающемся списке **Имя виртуального Сервера администрирования** выберите нужный виртуальный Сервер администрирования.

7. На шаге мастера **Выбор учетной записи для запуска задачи** укажите параметры учетной записи:

   Учетная запись по умолчанию

   Задача будет запускаться под той же учетной записью, под которой было установлено и запущено приложение, выполняющее эту задачу.

   По умолчанию выбран этот вариант.

   Задать учетную запись

   В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.

Учетная запись

Учетная запись, от имени которой будет запускаться задача.

Пароль

Пароль учетной записи, от имени которой будет запускаться задача.

8. Если требуется изменить параметры задачи по умолчанию, на шаге мастера **Завершение создания задачи** 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.

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. Если вы хотите изменить параметры задачи по умолчанию, в окне свойств задачи укажите общие параметры задачи в соответствии с вашими требованиями.

12. Нажмите на кнопку **Сохранить**.

    Задача создана и настроена.

13. Запустите созданную задачу.

После завершения работы задачи клиентские устройства, для которых она была создана, переходят под управление Сервера администрирования, указанного в параметрах задачи.

Удаление виртуального Сервера администрирования

При удалении виртуального Сервера администрирования все объекты, созданные на Сервере администрирования, включая политики и задачи, также будут удалены. Управляемые устройства из групп администрирования, которыми управлял виртуальный Сервер администрирования, будут удалены из групп администрирования. Чтобы вернуть устройства под управление Kaspersky Security Center Linux, выполните опрос сети, а затем переместите найденные устройства из группы Нераспределенные устройства в группы администрирования.

Чтобы удалить виртуальный Сервер администрирования:

1. Переключитесь на главный физический Сервер администрирования, которому принадлежит виртуальный Сервер администрирования:

   a. В главном меню выберите любой раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**.

   b. В открывшейся панели нажмите на имя нужного главного физического Сервера администрирования.

      В главном меню Сервер администрирования изменится на тот, который вы выбрали.

2. Перейдите к свойствам главного физического Сервера администрирования одним из следующих способов:

   - В панели наведите курсор мыши на название нужного Сервера администрирования и нажмите на значок параметров (⚙).
   - В главном окне приложения нажмите на имя Сервера администрирования.

3. В открывшемся окне свойств страницы выберите вкладку **Серверы администрирования**.

4. Выберите виртуальный Сервер администрирования, который вы хотите удалить.

5. В строке меню нажмите на кнопку **Удалить**.

   Виртуальный Сервер администрирования удален.

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 окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

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

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

   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, приложение вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400 000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

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

Когда Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий операционной системы. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления. 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 главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

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

3. Нажмите на кнопку **Сохранить**.

Также вы можете выполнить следующее:

- Изменить параметры любой задачи, чтобы сохранять события, связанные с ходом выполнения задачи, или сохранять только результаты выполнения задачи.

- Уменьшить или выключить период хранения для событий Сервера администрирования, Агента администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах.

Таким образом вы уменьшаете количество событий в базе данных, увеличиваете скорость работы сценариев, связанных с анализом таблицы событий в базе данных, и снижаете риск вытеснения критических событий большим количеством событий.

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 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 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 Linux). Если вам нужно сохранить сервер базы данных на предыдущем устройстве, введите IP-адрес предыдущего устройства в пункте "h" инструкции Установка Kaspersky Security Center Linux.

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

8. Откройте Kaspersky Security Center 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.

Смена имени Сервера администрирования

Действия при смене имени Сервера могут отличаться в зависимости от вашей среды. Вы можете выбрать один из следующих сценариев изменения имени Сервера:

- Сохранение подключений с помощью добавления новой записи DNS.
- Сохранение подключений с помощью переключения на основе IP-адреса.
- Восстановление прерванных подключений после изменения имени Сервера.

Если у вас возникли проблемы со сменой имени Сервера, обратитесь в Службу технической поддержки.

Сохранение подключений с помощью добавления новой записи DNS

В этом сценарии управляемые устройства и Kaspersky Security Center Web Console продолжат подключение к старому адресу Сервера администрирования после переименования Сервера администрирования. Чтобы настроить это, добавьте один из следующих типов записей DNS:

- Запись A для старого адреса Сервера администрирования, указывающая на новый IP-адрес Сервера администрирования.
- Запись CNAME, связывающая старое имя Сервера администрирования с новым именем Сервера администрирования.

  Дополнительную информацию о настройке требуемых записей см. в документации DNS-сервера.

Чтобы сохранить подключения с помощью добавления новой записи DNS:

1. **Измените имя Сервера.**

   Так как компоненты настроены во время установки, вы не можете изменить имя Сервера администрирования без переустановки Сервера администрирования.

   Чтобы изменить имя Сервера:

   1. Создайте новую резервную копию данных Сервера администрирования с помощью утилиты klbackup.
   2. Удалите Kaspersky Security Center Linux и Kaspersky Security Center Web Console со всех рабочих станций администраторов.
   3. Вручную удалите базу данных Сервера администрирования и базу данных IAM. Сервер администрирования не удаляет их автоматически при деинсталляции.
   4. Переименуйте устройство в операционной системе Сервера администрирования в соответствии с документацией вашей ОС.
   5. Установите Сервер администрирования Kaspersky Security Center Linux, используя новый FQDN Сервера администрирования.
   6. После установки восстановите ранее подготовленную резервную копию данных Сервера администрирования.
   7. Проверьте конфигурацию сервера IAM и, при необходимости, добавьте адрес Сервера администрирования в конфигурационный файл сервера IAM.
   8. Установите Web Console на все рабочие места администратора, указав новый FQDN Сервера администрирования в файле ответов.

2. Добавьте новую DNS-запись для старого адреса Сервера администрирования.
3. Укажите новый адрес в параметрах Сервера администрирования в Kaspersky Security Center Web Console.

4. Запустите задачу **Смена Сервера администрирования** на устройствах с прямым доступом Сервера администрирования. После этого управляемые устройства смогут подключаться к Серверу администрирования с новым именем.

   Не запускайте задачу на устройствах, у которых нет прямого доступа к Серверу, иначе они потеряют связь с Сервером администрирования и шлюзами соединения.

   Управляемые устройства, подключенные через шлюзы соединения, не проверяют имя Сервера администрирования. Поэтому никакие дополнительные действия с ними не требуются. Информация об адресе Сервера администрирования не будет обновляться в выводе диагностической команды klnagchk.

Подключение к Серверу администрирования сохраняется после изменения имени Сервера.

После изменения имени Сервера информация о сертификате устареет. Поскольку это не влияет на работу компонентов, не рекомендуется заменять самоподписанные сертификаты вне расписания. Эти сертификаты генерируются установщиком Kaspersky Security Center и автоматически обновляются Сервером. Сертификаты будут перевыпущены с новым именем Сервера администрирования при следующей автоматической замене сертификатов.

Во время переустановки будут выданы новые сертификаты для сервера IAM и Сервера Web Console. При необходимости замените их пользовательскими сертификатами, выданными вашим центром сертификации для нового имени Сервера администрирования. Подробнее см. в статье О сертификатах Kaspersky Security Center Linux.

Сохранение подключений с помощью переключения на основе IP-адреса

В этом сценарии изменяется способ подключения управляемых устройств к Серверу администрирования. Устройства подключаются с использованием IP-адреса Сервера администрирования вместо имени Сервера администрирования. Переключение всех управляемых устройств может занять время в зависимости от количества устройств и частоты их появления в сети с Сервером администрирования.

Чтобы сохранить соединения с помощью переключения на основе IP-адреса:

1. **Перед изменением имени Сервера администрирования подготовьте инфраструктуру Kaspersky Security Center.**

   1. Подключите управляемые устройства к Серверу администрирования с помощью IP-адреса. После изменения имени Сервера администрирования устройства, использующие его имя для подключения, будут отключены от Сервера. Чтобы подключиться через IP-адрес, запустите задачу Смена Сервера администрирования на устройствах с прямым доступом к Серверу администрирования, включая устройства, выступающие в роли шлюзов соединения.

      Не запускайте задачу на устройствах, у которых нет прямого доступа к Серверу, иначе они потеряют связь с Сервером администрирования и шлюзами соединения.

      Управляемые устройства, подключенные через шлюзы соединения, не проверяют имя Сервера администрирования. Поэтому никакие дополнительные действия с ними не требуются. Информация об адресе Сервера администрирования не будет обновляться в выводе диагностической команды klnagchk.

2. Убедитесь, что все управляемые устройства подключены к Серверу администрирования по IP-адресу. Для этого проверьте следующее:

   - Результаты диагностической команды klnagchk в строке "Адрес Сервера администрирования" на управляемых устройствах с прямым доступом к Серверу администрирования.
   - Информацию о свойствах инсталляционного пакета Агента администрирования на момент установки на устройства.

     Агент администрирования должен быть изначально настроен для подключения к Серверу администрирования по IP-адресу.

     > Если вы устанавливаете Агент администрирования поверх существующей установки, не удаляя ее предварительно, адрес подключения к Серверу администрирования и сертификат, указанные в конфигурации Агента администрирования, обновляться не будут.

3. Укажите новое имя в существующих профилях подключений к Серверу администрирования.
4. Если вы используете роль Управление мобильными устройствами (управление устройствами Android и iOS), следуйте инструкциям Как изменить адрес Сервера администрирования на мобильных устройствах, использующих Kaspersky Endpoint Security для Android с ролью MDM или KSMM.

2. **Измените имя Сервера.**

Так как компоненты настроены во время установки, вы не можете изменить имя Сервера администрирования без переустановки Сервера администрирования.

Чтобы изменить имя Сервера:

1. Создайте новую резервную копию данных Сервера администрирования с помощью утилиты klbackup.
2. Удалите Kaspersky Security Center Linux и Kaspersky Security Center Web Console со всех рабочих станций администраторов.
3. Вручную удалите базу данных Сервера администрирования и базу данных IAM. Сервер администрирования не удаляет их автоматически при деинсталляции.
4. Переименуйте устройство в операционной системе Сервера администрирования в соответствии с документацией вашей ОС.
5. Установите Сервер администрирования Kaspersky Security Center Linux, используя новый FQDN Сервера администрирования.
6. После установки восстановите ранее подготовленную резервную копию данных Сервера администрирования.
7. Проверьте конфигурацию сервера IAM и, при необходимости, добавьте адрес Сервера администрирования в конфигурационный файл сервера IAM.
8. Установите Web Console на все рабочие места администратора, указав новый FQDN Сервера администрирования в файле ответов.

3. **Обновите адреса Сервера администрирования в параметрах Сервера администрирования.**

   После изменения имени Сервера администрирования укажите новый FQDN-адрес в параметрах Сервера администрирования в Kaspersky Security Center Web Console. Для этого проверьте и обновите адрес FQDN в каждом из следующих параметров:

   - Адрес прокси-сервера Kaspersky Security Network.
   - Службу Веб-сервера.
   - Свойства инсталляционного пакета Агента администрирования.
   - Имя издателя кода безопасности (2FA).

   Также выполните следующие действия:

   - Укажите новое имя Сервера в политиках и параметрах других приложений "Лаборатории Касперского".
   - Повторно опубликуйте каждый опубликованный автономный пакет и пакет для мобильных устройств.
   - Переподключите подчиненные Серверы администрирования, если вы используете иерархию Серверов администрирования и если Серверы администрирования подключены по имени, а не по IP-адресу.

4. Запустите задачу **Смена Сервера администрирования** на устройствах с прямым доступом к Серверу администрирования, чтобы изменить адрес подключения на управляемых устройствах на новое имя Сервера администрирования.

Подключение к Серверу администрирования сохраняется после изменения имени Сервера.

После изменения имени Сервера информация о сертификате устареет. Поскольку это не влияет на работу компонентов, не рекомендуется заменять самоподписанные сертификаты вне расписания. Эти сертификаты генерируются установщиком Kaspersky Security Center и автоматически обновляются Сервером. Сертификаты будут перевыпущены с новым именем Сервера администрирования при следующей автоматической замене сертификатов.

Во время переустановки будут выданы новые сертификаты для сервера IAM и Сервера Web Console. При необходимости замените их пользовательскими сертификатами, выданными вашим центром сертификации для нового имени Сервера администрирования. Подробнее см. в статье О сертификатах Kaspersky Security Center Linux.

Восстановление прерванных подключений после изменения имени Сервера

Сценарий актуален в следующих случаях:

- Если вы потеряли право собственности на доменное имя устройства Сервера администрирования, но по-прежнему имеете доступ к Серверу администрирования.
- Если Сервер администрирования больше не управляет управляемыми устройствами.
- Если нет возможности добавить DNS-записи для старого адреса Kaspersky Security Center Linux по другим причинам.

Чтобы восстановить прерванные подключения после изменения имени Сервера:

1. **Измените имя Сервера.**

   Так как компоненты настроены во время установки, вы не можете изменить имя Сервера администрирования без переустановки Сервера администрирования.

   Чтобы изменить имя Сервера:

   1. Создайте новую резервную копию данных Сервера администрирования с помощью утилиты klbackup.
   2. Удалите Kaspersky Security Center Linux и Kaspersky Security Center Web Console со всех рабочих станций администраторов.
   3. Вручную удалите базу данных Сервера администрирования и базу данных IAM. Сервер администрирования не удаляет их автоматически при деинсталляции.
   4. Переименуйте устройство в операционной системе Сервера администрирования в соответствии с документацией вашей ОС.
   5. Установите Сервер администрирования Kaspersky Security Center Linux, используя новый FQDN Сервера администрирования.
   6. После установки восстановите ранее подготовленную резервную копию данных Сервера администрирования.
   7. Проверьте конфигурацию сервера IAM и, при необходимости, добавьте адрес Сервера администрирования в конфигурационный файл сервера IAM.
   8. Установите Web Console на все рабочие места администратора, указав новый FQDN Сервера администрирования в файле ответов.

2. **Обновите адреса Сервера администрирования в параметрах Сервера администрирования.**

   После изменения имени Сервера администрирования укажите новый FQDN-адрес в параметрах Сервера администрирования в Kaspersky Security Center Web Console. Для этого проверьте и обновите адрес FQDN в каждом из следующих параметров:

   - Адрес прокси-сервера Kaspersky Security Network.
   - Службу Веб-сервера.
   - Свойства инсталляционного пакета Агента администрирования.
   - Имя издателя кода безопасности (2FA).

   Также выполните следующие действия:

   - Укажите новое имя Сервера в политиках и параметрах других приложений "Лаборатории Касперского".
   - Повторно опубликуйте каждый опубликованный автономный пакет и пакет для мобильных устройств.
   - Переподключите подчиненные Серверы администрирования, если вы используете иерархию Серверов администрирования и если Серверы администрирования подключены по имени, а не по IP-адресу.

3. Восстановите подключение к Серверу администрирования на ранее управляемых устройствах:

   - На устройствах с прямым доступом к Серверу администрирования используйте утилиту klmover, чтобы указать адрес подключения к Серверу администрирования с новым именем. Подробнее см. в статье: Подключение Агентов администрирования к Серверу администрирования с помощью утилиты klmover.

   - На устройствах, выступающих в роли шлюзов соединения, переустановите Агент администрирования и перенастройте роль шлюза соединения. Подробнее см. в статье Добавление шлюза соединения в демилитаризованной зоне в качестве точки распространения.

   - Устройства, подключенные через шлюзы соединения, будут автоматически переподключаться после восстановления шлюзов соединения. Агент администрирования не использует имя Сервера администрирования при подключении к шлюзу соединения.

     Не используйте утилиту klmover на устройствах, подключенных через шлюзы соединения. Подробнее см. в статье Перемещение устройств, подключенных к Серверу администрирования через шлюзы соединения, на другой Сервер администрирования.

Подключение к Серверу администрирования восстанавливается после изменения имени Сервера.

После изменения имени Сервера информация о сертификате устареет. Поскольку это не влияет на работу компонентов, не рекомендуется заменять самоподписанные сертификаты вне расписания. Эти сертификаты генерируются установщиком Kaspersky Security Center и автоматически обновляются Сервером. Сертификаты будут перевыпущены с новым именем Сервера администрирования при следующей автоматической замене сертификатов.

Во время переустановки будут выданы новые сертификаты для сервера IAM и Сервера Web Console. При необходимости замените их пользовательскими сертификатами, выданными вашим центром сертификации для нового имени Сервера администрирования. Подробнее см. в следующей статье: О сертификатах Kaspersky Security Center Linux.

Изменение учетных данных СУБД

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

Изменение учетных данных базы данных Сервера администрирования

Чтобы изменить учетные данные базы данных Сервера администрирования и базы данных IAM в среде Linux:

1. Остановите Сервер администрирования. В зависимости от типа развертывания Kaspersky Security Center Linux под учетной записью root выполните одну из следующих команд:

   - Для отказоустойчивого кластера Kaspersky Security Center Linux:

     На активном узле выполните следующую команду:

     ```
     /opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc
     ```

- Для георазпределенного отказоустойчивого кластера Kaspersky Security Center Linux:

  На обоих узлах выполните следующую команду:

  ```
  crm node standby
  ```

- Для развертывания Сервера администрирования не кластерной конфигурации:

  Выполните следующие команды:

  ```
  systemctl stop kladminserver_srv.service
  systemctl stop kliam_srv.service
  ```

2. Подключитесь к базе данных Сервера администрирования с правами суперпользователя СУБД и выполните следующую команду:

   ```
   REASSIGN OWNED BY <old_kscdbadmin> TO <new_kscdbadmin>;
   ```

   где `<old_kscdbadmin>` – предыдущая учетная запись СУБД, которую Сервер администрирования использовал для подключения к своей базе данных, а `<new_kscdbadmin>` – новая учетная запись СУБД.

3. Подключитесь к базе данных IAM с правами суперпользователя СУБД и выполните следующую команду:

   ```
   REASSIGN OWNED BY <old_iamdbadmin> TO <new_iamdbadmin>;
   ```

   где `<old_iamdbadmin>` – предыдущая учетная запись СУБД, которую Сервер администрирования использовал для подключения к своей базе данных, и `<new_iamdbadmin>` – это новые учетные записи СУБД.

4. Откройте конфигурационный файл IAM /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml.

5. В секции `dbms_iam` укажите новые учетные данные в полях user и password. Убедитесь, что учетная запись существует в СУБД и указана как владелец базы данных IAM.

6. Запустите Сервер администрирования. В зависимости от типа развертывания Kaspersky Security Center Linux под учетной записью root выполните одну из следующих команд:

   - Для отказоустойчивого кластера Kaspersky Security Center Linux:

     На активном узле выполните следующую команду:

     ```
     /opt/kaspersky/ksc64/sbin/klfoc -startcluster --stp klfoc
     ```

   - Для георазпределенного отказоустойчивого кластера Kaspersky Security Center Linux:

     На обоих узлах выполните следующую команду:

     ```
     crm node online
     ```

- Для развертывания Сервера администрирования не кластерной конфигурации:

  Выполните следующие команды:

  ```
  systemctl start kladminserver_srv.service
  systemctl start kliam_srv.service
  ```

7. Запустите утилиту klsrvconfig:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```

8. Укажите новое имя учетной записи. Вам нужно указать учетные данные учетной записи, которая существует в СУБД.

9. Введите новый пароль.

10. Укажите этот новый пароль для подтверждения.

11. Дождитесь возобновления работы Сервера администрирования и появления записи в syslog о том, что Сервер администрирования готов к работе с графическим интерфейсом пользователя.

Учетные данные базы данных Сервера администрирования изменены.

Резервное копирование и восстановление данных Сервера администрирования

Резервное копирование данных позволяет переносить Сервер администрирования с одного устройства на другое без потерь информации. С помощью резервного копирования вы можете восстанавливать данные при переносе информационной базы Сервера администрирования на другое устройство или при переходе на более позднюю версию Kaspersky Security Center. Также вы можете использовать резервное копирование данных для переноса данных Сервера администрирования Kaspersky Security Center Windows под управление Kaspersky Security Center Linux (перенос данных из Kaspersky Security Center Linux в Kaspersky Security Center Windows не поддерживается).

Резервные копии установленных плагинов управления не сохраняются. После восстановления данных Сервера администрирования из резервной копии необходимо загрузить и переустановить плагины управляемых приложений.

Перед созданием резервной копии данных Сервера администрирования выполните следующие действия:

- **Обеспечьте соблюдение требований для создания резервной копии на Сервере администрирования версии 16 или ниже и восстановления на Сервере администрирования версии 16.1 или выше.**

  - Если резервная копия данных создается на Сервере администрирования версии 16 или ниже, а восстановление из нее выполняется на Сервере администрирования версии 16.1 или выше, двухфакторная аутентификация будет включена. Дополнительные сведения см. в статье О двухфакторной аутентификации учетной записи.

Чтобы обеспечить вход пользователей в Web Console с прежними учетными записями с помощью настроенных секретных ключей двухфакторной аутентификации, а скрипты автоматизации OpenAPI продолжали работать после восстановления, необходимо выполнить следующие действия:

- Включение двухфакторной аутентификации для всех пользователей
- Администраторы должны настроить двухфакторную аутентификацию для собственных учетных записей
- Исключение учетных записей из двухфакторной аутентификации

  Если требуется, добавьте учетные записи интеграций, используемые для запуска скриптов через OpenAPI, в список исключений.

Если невозможно настроить двухфакторную аутентификацию перед созданием резервной копии, учетные записи добавляются в список разрешений для настройки двухфакторной аутентификации, и пользователи смогут настроить двухфакторную аутентификацию при входе в Web Console. Дополнительные сведения об условиях добавления учетной записи в список разрешений для настройки двухфакторной аутентификации описаны в разделе Разрешение для настройки двухфакторной аутентификации пользователям.

- 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.

- Если резервное копирование или восстановление выполняется для отказоустойчивого кластера Kaspersky Security Center Linux, необходимо остановить весь кластер для технического обслуживания, а затем перезагрузить его после завершения резервного копирования или восстановления.

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

- Создать и запустить задачу резервного копирования данных через Kaspersky Security Center Web Console.

- 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 приложения (обычно, /opt/kaspersky/ksc64/sbin/klbackup).

В резервной копии данных Сервера администрирования сохраняются следующие данные:

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

- конфигурационная информация о структуре групп администрирования и клиентских устройствах;

- хранилище дистрибутивов приложений для удаленной установки;

- сертификат Сервера администрирования;

- секретные ключи двухфакторной аутентификации, настроенные для учетных записей пользователей;
- список учетных записей, исключенных из двухфакторной аутентификации.

Создать резервную копию данных Сервера администрирования можно либо путем создания и выполнения задачи резервного копирования данных, либо с помощью утилиты klbackup. Восстановление данных Сервера администрирования возможно только с помощью утилиты klbackup. Вам нужно выполнить восстановление на только что установленном и работоспособном экземпляре Сервера администрирования той версии, для которой была сделана резервная копия (или более новой). Не используйте какие-либо сторонние инструменты для резервного копирования или восстановления и, если возможно, не удаляйте предыдущую установку Kaspersky Security Center Linux до тех пор, пока настройка и перенос данных не будут полностью завершены.

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. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В списке **Приложение** выберите **Kaspersky Security Center 17** 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.

Экземпляр Сервера администрирования, на который выполняется восстановление, должен использовать СУБД того же типа. Версия Сервера администрирования может быть той же самой (с аналогичным или более новым патчем) или более новой.

Если вы выполнили резервное копирование данных Сервера администрирования, входящего в состав Kaspersky Security Center Linux 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 <путь к резервной копии> [-linux_path <путь к резервной копии СУБД>-
node_cert <путь к сертификату>] [-logfile <файл журнала> [-use_ts]|[-restore] [-
password <пароль>] [-cert_only]
```

Если не задать пароль в командной строке утилиты klbackup, утилита запросит его ввод интерактивно.

Описания ключей:

- `-path <путь к резервной копии>` – сохранять информацию в папке резервной копии или использовать для восстановления данные из папки к резервной копии (обязательный параметр).
- `-linux_path <путь к резервной копии СУБД>` – 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 резервной копии СУБД.
- `-node_cert <путь к сертификату>` – файл сертификата Сервера для настройки пассивного узла отказоустойчивого кластера после восстановления. Если параметр не указан, он будет автоматически получен с Сервера.

- `-logfile <файл журнала>` – сохранять отчет о копировании или восстановлении данных Сервера администрирования.

  Учетная запись сервера базы данных и утилита klbackup должны обладать правами на изменение данных в папке резервной копии.

- `-use_ts` – при сохранении данных копировать информацию в папку резервной копии, во вложенную папку с именем в формате `klbackup ГГГГ-ММ-ДД # ЧЧ-ММ-СС`, включающем текущие дату и время операции в формате UTC. Если ключ не задан, информация сохраняется в корне папки резервной копии.

  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 резервной копии. Если ключ отсутствует, производится резервное копирование данных в папку резервной копии.

- `-password <пароль>` – 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.

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

  Этот флаг может быть полезен при выполнении переноса данных с Сервера администрирования Kaspersky Security Center Windows на Сервер администрирования Kaspersky Security Center Linux. Также вы можете переносить управляемые устройства между Серверами администрирования Kaspersky Security Center Linux и между Серверами администрирования Kaspersky Security Center Windows.

Вы можете использовать резервное копирование данных, чтобы переместить данные Сервера администрирования Kaspersky Security Center Windows под управление Kaspersky Security Center Linux.
Если вы используете MySQL или MariaDB в качестве СУБД для Kaspersky Security Center Windows и для Kaspersky Security Center Linux, параметр `lower_case_table_names` должен совпадать в текущей и новой СУБД.
Перед созданием резервной копии данных проверьте параметр `lower_case_table_names`. Затем при установке MySQL или MariaDB для Kaspersky Security Center Linux, вам нужно установить то же значение параметра `lower_case_table_names`, которое указано для этого параметра для Windows.

Если при восстановлении общий сертификат Сервера администрирования заменяется другим сертификатом из резервной копии, выполните следующие действия, чтобы обеспечить правильную работу:
1. Переустановите Web Console, чтобы избежать следующей ошибки:
Сервер администрирования использует недоверенный сертификат. Перенастройте приложение, указав действительный сертификат, или обратитесь к главному администратору.
2. Проверьте конфигурацию сервера IAM и, при необходимости, добавьте адрес Сервера администрирования в конфигурационный файл сервера IAM.

Использование утилиты klbackup для переключения управляемых устройств под управление другого Сервера администрирования

Утилита klbackup позволяет переключать управляемые устройства под управление другого Сервера администрирования. Вы можете сменить Сервер администрирования Kaspersky Security Center Windows на Сервер администрирования Kaspersky Security Center Linux, используя утилиту klbackup, при выполнении переноса данных. Также вы можете переносить управляемые устройства между Серверами администрирования Kaspersky Security Center Linux и между Серверами администрирования Kaspersky Security Center Windows.

Прежде чем начать, **проверьте требования к пользовательскому сертификату**.

Если вы используете пользовательский сертификат вместо самоподписанного, перед обновлением Kaspersky Security Center Linux до более поздней версии вам нужно убедиться, что сертификат содержит альтернативное имя субъекта (Subject Alternative Name, SAN). Если нет, важно заменить сертификат перед обновлением Kaspersky Security Center Linux. Иначе вы не сможете войти в Web Console после обновления.

Чтобы убедиться, что сертификат включает SAN:

1. На устройстве, на котором установлен Сервер администрирования, выполните команду:

   - Для устройств с операционной системой Linux:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - Для устройств с операционной системой Windows:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Убедитесь, что альтернативное имя субъекта (SAN) присутствует в выходных данных команды и содержит адрес устройства Сервера администрирования.

3. Если альтернативное имя субъекта отсутствует, используйте утилиту klsetsrvcert для замены пользовательского сертификата на сертификат, который соответствует требованиям.

Чтобы переключить управляемые устройства под управление другого Сервера администрирования с помощью утилиты klbackup:

1. На предыдущем устройстве создайте резервную копию сертификата и закрытого ключа Сервера администрирования.

Вы можете создать резервную копию данных одним из следующих способов:

- С помощью интерфейса утилиты klbackup (только для Сервера администрирования Kaspersky Security Center Windows).

  Запустите утилиту klbackup, расположенную в папке установки Kaspersky Security Center, а затем создайте резервную копию с помощью параметра **Выполнять резервное копирование и восстановление только для сертификата Сервера администрирования**.

- С помощью командной строки (для Серверов администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux версии 15.1 и выше).

  Запустите утилиту klbackup с ключом `-cert_only` из командной строки, чтобы создать резервную копию сертификата и закрытого ключа Сервера администрирования:

  ```
  klbackup -path <path to the backup copy of Administration Server certificate> -cert_only
  ```

2. На предыдущем устройстве отключите Сервер администрирования от сети.

3. Присвойте устройству такое же доменное имя, как и другому Серверу администрирования.

   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).

   Если невозможно назначить тот же адрес для устройства с другим Сервером администрирования, нужно сгенерировать новый сертификат Сервера администрирования и указать этот сертификат в конфигурационном файле IAM. После установки Сервера администрирования вам нужно вручную переключить Агенты администрирования на новый Сервер администрирования.

4. На устройстве с другим Сервером администрирования восстановите сертификат Сервера администрирования и закрытый ключ из резервной копии.

   Вы можете восстановить резервную копию данных одним из следующих способов:

   - С помощью интерфейса утилиты klbackup (только для Сервера администрирования Kaspersky Security Center Windows).

     Запустите утилиту klbackup и восстановите резервную копию, используя параметр **Выполнять резервное копирование и восстановление только для сертификата Сервера администрирования**.

   - С помощью командной строки (для Серверов администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux версии 15.1 и выше).

     Запустите утилиту `klbackup` с ключом `-cert_only` из командной строки, чтобы восстановить резервную копию сертификата и закрытого ключа Сервера администрирования:

     ```
     klbackup -path <path to the backup copy of Administration Server certificate> -restore -cert_only
     ```

5. Настройте проверку сертификата Сервером администрирования и сервером IAM.

Управляемые устройства перейдут под управление другого Сервера администрирования. Вы можете перейти на Сервер администрирования и убедиться, что управляемые устройства видны в сети и что на них установлен и запущен Агент администрирования (значение *Да* в столбцах **Видимо в сети**, **Агент администрирования установлен** и **Агент администрирования запущен**).

Резервное копирование и восстановление данных Сервера администрирования при использовании MySQL или MariaDB

Вы можете использовать резервное копирование данных, чтобы перенести данные Сервера администрирования из Kaspersky Security Center Windows под управление Kaspersky Security Center Linux. Перенос данных с использованием резервной копии данных Сервера администрирования поддерживается только для переноса в Kaspersky Security Center Linux 15.2 или более позднюю версию из любой поддерживаемой версии Kaspersky Security Center Windows.

Если вы используете MySQL или MariaDB в качестве СУБД для Kaspersky Security Center Windows и для Kaspersky Security Center Linux, параметр `lower_case_table_names` должен совпадать в текущей и новой СУБД. Иначе данные Сервера администрирования будут перенесены некорректно.

Прежде чем вы создадите резервную копию данных Сервера администрирования Kaspersky Security Center Windows, проверьте значение параметра `lower_case_table_names`. Если вы не указали этот параметр ранее во время установки СУБД, используется значение параметра по умолчанию. Значение параметра `lower_case_table_names` по умолчанию для Windows – `1`.

При установке MySQL или MariaDB для Kaspersky Security Center Linux установите то же значение параметра `lower_case_table_names`, которое указано для этого параметра для Windows. Подробнее см. инструкцию с веб-сайта MySQL. Если вы не указали этот параметр, используется значение параметра по умолчанию. Для операционных систем на основе Linux значение параметра `lower_case_table_names` по умолчанию отличается от значения по умолчанию для Windows.

Если вы хотите установить MySQL 8.0, параметр `lower_case_table_names`, который задан в соответствии с этой инструкцией может, не сработать. В этом случае сначала вам нужно установить MySQL 5.7, указать параметр `lower_case_table_names`, как описано в инструкции, а затем обновить MySQL 5.7 до MySQL 8.0. Если параметр `lower_case_table_names` не совпадает в текущей и новой СУБД, данные Сервера администрирования будут восстановлены некорректно.

Обслуживание Сервера администрирования

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

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

- Удаляет ненужные папки и файлы из папки хранилища.
- Удаляет ненужные записи из таблиц (также известные как "висячие указатели").
- Очищает кеш.

- Обслуживает базу данных (если в качестве СУБД используется PostgreSQL):
  - перестраивает индексы базы данных;
  - обновляет статистику базы данных;
  - сжимает базу данных (если необходимо).

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

Задача Обслуживание Сервера администрирования создается автоматически при запуске Сервера администрирования. Если задача Обслуживание Сервера администрирования удалена, вы можете создать ее вручную.

Чтобы создать задачу Обслуживание Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

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

В результате созданная задача отобразится в списке задач. Для одного Сервера администрирования может выполняться только одна задача Обслуживание Сервера администрирования. Если задача Обслуживание Сервера администрирования для Сервера администрирования уже создана, создание еще одной задачи Обслуживание Сервера администрирования невозможно.

Удаление иерархии Серверов администрирования

Если вам больше не нужна иерархия Серверов администрирования, вы можете отключить их от этой иерархии.

Чтобы удалить иерархию Серверов администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.
2. На открывшейся странице перейдите на вкладку **Серверы администрирования**.
3. В группе администрирования, в которой вы хотите удалить подчиненный Сервер администрирования, выберите подчиненный Сервер администрирования.

4. В меню выберите пункт **Удалить**.

5. В открывшемся окне нажмите на кнопку **ОК** для подтверждения удаления подчиненного Сервера администрирования.

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

Доступ к общедоступным DNS-серверам

Если доступ к серверам "Лаборатории Касперского" через системный DNS невозможен, Kaspersky Security Center Linux может использовать публичные DNS-серверы в следующем порядке:

1. Google Public DNS (8.8.8.8).

2. Cloudflare DNS (1.1.1.1).

3. Alibaba Cloud DNS (223.6.6.6).

4. Quad9 DNS (9.9.9.9).

5. CleanBrowsing (185.228.168.168).

Запросы к этим DNS-серверам могут содержать доменные адреса и общедоступный IP-адрес Сервера администрирования, так как приложение устанавливает TCP/UDP-соединение с DNS-сервером. Если Kaspersky Security Center Linux использует общедоступный DNS-сервер, обработка данных регулируется политикой конфиденциальности соответствующего сервиса.

Чтобы настроить использование публичного DNS с помощью утилиты klscflag:

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

2. Чтобы выключить использование публичного DNS, выполните следующую команду под учетной записью root:

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

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

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

Настройка интерфейса

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

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

1. В главном окне приложения перейдите в раздел **Параметры** → **Параметры интерфейса**.
2. Включите или выключите нужные параметры:
   - **Показать раздел "Шифрование и защита данных"**
   - **Показать функции MDR**
   - **Показать EDR-алерты**
3. Нажмите на кнопку **Сохранить**.

После включения нужных параметров Консоль отображает соответствующие разделы в главном меню. Например, если включить **Показать EDR-алерты**, раздел **Мониторинг** → **Алерты** появится в главном меню.

Защищенное подключение к Серверу администрирования

Обмен информацией между клиентскими устройствами и Сервером администрирования могут производиться с использованием протокола TLS (Transport Layer Security). Протокол TLS позволяет идентифицировать стороны, взаимодействующие при подключении, осуществлять шифрование передаваемых данных и обеспечивать их защиту от изменения при передаче. В основе протокола TLS лежит аутентификация взаимодействующих сторон и шифрование данных по методу открытых ключей.

При первом подключении клиентского устройства к Серверу администрирования Агент администрирования на устройстве получает копию сертификата Сервера администрирования и сохраняет его локально.

При локальной установке Агента администрирования на устройство сертификат Сервера администрирования можно выбрать вручную.

На основании полученной копии сертификата осуществляется проверка прав и полномочий Сервера администрирования при следующих соединениях.

В дальнейшем, при каждом подключении устройства к Серверу администрирования Агент администрирования запрашивает сертификат Сервера администрирования и сравнивает его с локальной копией. Если они не совпадают, доступ Сервера администрирования к устройству не разрешается.

Шифрование подключения TLS

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

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

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

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

2. Используйте флаг SrvUseStrictSslSettings, чтобы настроить разрешенные протоколы шифрования и наборы шифрования на Сервере администрирования. Выполните следующую команду в командной строке под учетной записью root:

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

   Укажите параметр <value> флага SrvUseStrictSslSettings:

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

     Наборы шифрования поддерживаемые TLS-протоколом 1.2:

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

     Наборы шифрования поддерживаемые TLS-протоколом 1.3:

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

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

     Наборы шифрования поддерживаемые TLS-протоколом 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384

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

Наборы шифрования поддерживаемые TLS-протоколом 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

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

3. Перезапустите следующие службы Kaspersky Security Center Linux:
   - службу Сервера администрирования;
   - службу Веб-сервера;
   - службу активации прокси-сервера.

В результате включается шифрование трафика с помощью TLS-протокола.

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

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

1. Запустите утилиту klscflag.

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

2. Выполните одну из следующих команд в командной строке под учетной записью root:
   - Используйте эту команду, чтобы включить или выключить поддержку TLS-протокола 1.2:

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

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

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

Укажите параметр < значение > флага:

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

Сетевые параметры для взаимодействия с внешними сервисами

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

Сетевые параметры

Сетевые параметры	Адрес	Описание
Порт: 443 Протокол: HTTPS	`https://activation-v2.kaspersky.com`	Активация приложения.
Port: 443 Protocol: HTTPS	`https://products.s.kaspersky-labs.com`	Хранилище дистрибутивов приложений для удаленной установки.

Порт: 443
Протокол: HTTPS
	`https://s00.upd.kaspersky.com`
	`https://s01.upd.kaspersky.com`
	`https://s02.upd.kaspersky.com`
	`https://s03.upd.kaspersky.com`
	`https://s04.upd.kaspersky.com`
	`https://s05.upd.kaspersky.com`
	`https://s06.upd.kaspersky.com`
	`https://s07.upd.kaspersky.com`
	`https://s08.upd.kaspersky.com`
	`https://s09.upd.kaspersky.com`
	`https://s10.upd.kaspersky.com`
	`https://s11.upd.kaspersky.com`
	`https://s12.upd.kaspersky.com`
	`https://s13.upd.kaspersky.com`
	`https://s14.upd.kaspersky.com`
	`https://s15.upd.kaspersky.com`
	`https://s16.upd.kaspersky.com`
	`https://s17.upd.kaspersky.com`
	`https://s18.upd.kaspersky.com`
	`https://s19.upd.kaspersky.com`
	`https://cm.k.kaspersky-labs.com`
		Обновление баз, модулей приложений и приложений "Лаборатории Касперского".

Порт: 443 Протокол: HTTPS	`https://downloads.upd.kaspersky.com`	• Обновление баз, модулей приложений и приложений "Лаборатории Касперского". • Проверка если серверы "Лаборатории Касперского" доступны. Kaspersky Security Center Linux проверяет доступность серверов "Лаборатории Касперского" перед загрузкой баз и модулей приложений "Лаборатории Касперского". Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы.

Сетевые параметры	Адрес	Описание
Порт: 80 Протокол: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	Обновление баз, модулей приложений и приложений "Лаборатории Касперского".
Порт: 443 Протокол: HTTPS	https://ds.kaspersky.com https://dc1.ksn.kaspersky-labs.com https://dc1-file.ksn.kaspersky-labs.com https://dc1-pp.ksn.kaspersky-labs.com https://dc1-st.ksn.kaspersky-labs.com/ https://dc1-cert.ksn.kaspersky-labs.com https://dc1-cf.ksn.kaspersky-labs.com https://dc1-file.ksn.kaspersky-labs.com https://dc1-kas.ksn.kaspersky-labs.com https://dc1-ml.ksn.kaspersky-labs.com https://dc1-pp.ksn.kaspersky-labs.com https://dc1-st.ksn.kaspersky-labs.com https://dc1.ksn.kaspersky-labs.com	Использование Kaspersky Security Network.

Сетевые параметры	Адрес	Описание
Порт: 443, 1443 Протокол: HTTPS	https://ksn-file-geo.kaspersky-labs.com https://ksn-verdict-geo.kaspersky-labs.com https://ksn-url-geo.kaspersky-labs.com https://ksn-a-p2p-geo.kaspersky-labs.com https://ksn-info-geo.kaspersky-labs.com https://ksn-cinfo-geo.kaspersky-labs.com	Использование Kaspersky Security Network.
Порт: 443, 1443 Протокол: KSN	ksn://ksn-a-p2p-geo.kaspersky-labs.com ksn://ksn-a-stat-geo.kaspersky-labs.com ksn://ksn-ca-geo.kaspersky-labs.com ksn://ksn-cinfo-geo.kaspersky-labs.com ksn://ksn-crypto-catm-geo.kaspersky-labs.com ksn://ksn-crypto-dnscheck-geo.kaspersky-labs.com ksn://ksn-crypto-hash-geo.kaspersky-labs.com ksn://ksn-crypto-ipm-geo.kaspersky-labs.com ksn://ksn-crypto-whocalls-geo.kaspersky-labs.com ksn://ksn-crypto-wifiplus-geo.kaspersky-labs.com ksn://ksn-eu-stat-kmp.kaspersky-labs.com ksn://ksn-file-geo.kaspersky-labs.com ksn://ksn-his-geo.kaspersky-labs.com ksn://ksn-info-geo.kaspersky-labs.com ksn://ksn-kas-geo.kaspersky-labs.com ksn://ksn-kddi.kaspersky-labs.com ksn://ksn-ml-geo.kaspersky-labs.com ksn://ksn-oui-geo.kaspersky-labs.com ksn://ksn-pp.kaspersky-labs.com ksn://ksn-src.kaspersky-labs.com ksn://ksn-stat-geo.kaspersky-labs.com ksn://ksn-tcert-geo.kaspersky-labs.com ksn://ksn-url-geo.kaspersky-labs.com ksn://ksn-verdict-geo.kaspersky-labs.com ksn://mdr.ksn.kaspersky-labs.com ksn://stat-eu.ksn.kaspersky-labs.com ksn://stat-hq.ksn.kaspersky-labs.com ksn://stat-ru.ksn.kaspersky-labs.com ksn://stat-sa.ksn.kaspersky-labs.com ksn://stat-sbr.ksn.kaspersky-labs.com	Использование Kaspersky Security Network.

Сетевые параметры	Адрес	Описание
Порт: 443 Протокол: HTTPS	`https://click.kaspersky.com` `https://redirect.kaspersky.com`	Переход по ссылкам из интерфейса.
Порт: 80 Протокол: HTTP	`http://crl.kaspersky.com` `http://ocsp.kaspersky.com`	Эти серверы являются частью инфраструктуры открытых ключей (PKI) и необходимы для проверки статуса действительности сертификатов цифровой подписи "Лаборатории Касперского". CRL является списком отозванных сертификатов. OCSP позволяет запрашивать статус конкретного сертификата в режиме реального времени. Эти службы помогают обеспечить безопасность взаимодействия с цифровыми сертификатами и защитить от возможных атак.
Порт: 443 Протокол: HTTPS	`https://ipm-klca.kaspersky.com`	Рекламные объявления.
Порт: 443 Протокол: HTTPS	`https://tip.kaspersky.com`	Реагирование на угрозы с помощью Kaspersky Threat Intelligence Portal (с использованием функциональности Kaspersky Security для бизнеса Профессиональный).
Порт: 443 Протокол: HTTPS	Полный список адресов см. в статье Структура адресов и доменов	Реагирование на угрозы с помощью Kaspersky Automated Security Awareness Platform (с использованием функциональности Kaspersky Security для бизнеса Профессиональный).

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

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

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

2. Если вы хотите загружать обновления по протоколу HTTP, выполните одну из следующих команд под учетной записью root:

   - На устройстве, на котором установлен Сервер администрирования:

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

   - На точку распространения:

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

   Если вы хотите загружать обновления по протоколу HTTPS, выполните одну из следующих команд под учетной записью root:

   - На устройстве, на котором установлен Сервер администрирования:

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

   - На точку распространения:

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

Глобальный список подсетей

Для каждого используемого вами Сервера администрирования можно настроить глобальный список подсетей для хранения информации о подсетях вашей сети. Этот список позволит сопоставить пары {IP-адрес, маска} и физические единицы, такие как офисы филиалов. Вы можете использовать подсети из этого списка в сетевых правилах и параметрах.

Чтобы добавить подсеть в глобальный список подсетей:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Глобальные подсети**.

3. Нажмите на кнопку **Добавить**.

   Откроется окно **Новая подсеть**.

4. Заполните следующие поля:

   - **Имя**
   - **Адрес подсети**
   - **Маска подсети**
   - **Описание**

5. Нажмите на кнопку **Сохранить**.

Подсеть появится в списке подсетей.

При необходимости в списке глобальных подсетей вы можете выполнить следующие действия:

- Удалить подсети из списка, выбрав нужную подсеть и нажав на кнопку **Удалить**.
- Изменить свойства подсетей, нажав на название нужной подсети и выполнив действия, описанные в шагах 4–5.

Проверка целостности модулей с помощью утилит klscmodchk и integrity_checker

Kaspersky Security Center Linux содержит двоичные модули в виде динамически подключаемых библиотек, исполняемых файлов, конфигурационных файлов и файлов интерфейса. Злоумышленники могут заменить один или несколько исполняемых модулей или файлов приложений другими файлами, содержащими вредоносный код. Для предотвращения подмены модулей и файлов в Kaspersky Security Center Linux реализована проверка целостности компонентов с помощью утилит klscmodchk и integrity_checker. Эти утилиты проверяют модули и файлы на предмет несанкционированных изменений или повреждений. Если модуль или файл приложения имеют неверную контрольную сумму, они считаются поврежденными.

Утилита klscmodchk выполняет проверку целостности следующих компонентов Kaspersky Security Center Linux:

- Сервер администрирования
- Агент администрирования

Утилита integrity_checker выполняет проверку целостности следующих компонентов Kaspersky Security Center Linux:

- Сервер администрирования
- Агент администрирования
- Kaspersky Security Center Web Console

Обе утилиты проверяют целостность модуля на основе файла манифеста kl_file_integrity_manifest.xml, который входит в сборку Kaspersky Security Center Linux и находится в папке установки. Файл манифеста компонента содержит файлы, целостность которых важна для корректной работы компонента Kaspersky Security Center Linux. Также проверяется целостность самих файлов манифеста.

Настоятельно не рекомендуется изменять файл манифеста kl_file_integrity_manifest.xml, так как цифровая подпись будет недействительна и это приведет к сбою проверки целостности.

Чтобы проверить целостность компонента Kaspersky Security Center Linux, выполните одну из следующих команд:

- `klscmodchk [ параметры ]`

  Утилита klscmodchk запускает утилиту integrity_checker с параметром `--verbose` и проверяет целостность модулей.

  Параметры утилиты klscmodchk:

  - `-logfile < путь_к_файлу_журнала >` – задает путь к файлу на диске для ведения журнала. По умолчанию информация выводится на консоли.
  - `-verbose` – отображает расширенную информацию во время проверки целостности.

- `integrity_checker [ параметры ] < путь_к_файлу_манифеста >`

  Параметры утилиты integrity_checker:

  - `--help` – отображает справку утилиты integrity_checker.
  - `--version` – отображает версию утилиты integrity_checker.
  - `--verbose` – отображает информацию о работе утилиты. При выполнении проверки целостности достаточно использовать этот параметр в команде.

Результат проверки каждого файла манифеста отображается рядом с именем файла манифеста в следующем формате:

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

Вы также можете настроить автоматический запуск проверки целостности при запуске приложения. По умолчанию автоматическая проверка целостности выключена.

Чтобы включить автоматическую проверку целостности:

1. На устройстве, на котором установлен Сервер администрирования, в командной строке выполните следующую команду:

   ```
   ./klscflag -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. Перезагрузите устройство.

   Автоматическая проверка целостности будет включена.

При следующем запуске Kaspersky Security Center утилита klscmodchk запустится вместе с Сервером администрирования и запустит проверку целостности модулей. Результат проверки целостности записывается в журнал Kaspersky Event Log.

Обнаружение устройств в сети

В этом разделе описаны поиск устройств и опрос сети.

Kaspersky Security Center Linux 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 и его подчиненных Серверов администрирования;
- нераспределенные устройства под управлением Сервера администрирования и его подчиненных Серверов администрирования.

Сценарий: обнаружение сетевых устройств

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

Обнаружение сетевых устройств состоит из следующих этапов:

1. **Первоначальное обнаружение устройств**

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

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 периодичности опросов сети.

   Также можно включить опрос Zeroconf, если в вашей сети есть IPv6-устройства.

   Если сетевые устройства включены в домен, рекомендуется использовать опрос контроллеров домена.

   Используйте точки распространения с операционной системой Windows для опроса сетей Windows.

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 сети Windows

Об опросе сети Windows

Сервер администрирования Kaspersky Security Center Linux не поддерживает опрос сети Windows. Используйте точки распространения с операционной системой Windows для опроса сетей Windows.

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

- имя операционной системы;
- IP-адрес;
- DNS-имя;
- NetBIOS-имя.

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

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

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

Опрос IP-диапазонов

Kaspersky Security Center Linux 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 Linux. 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 Linux 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 Linux автоматически включит сеть 192.168.0.0/24 в список адресов для опроса. Kaspersky Security Center Linux выполнит опрос всех адресов от 192.168.0.1 до 192.168.0.254.

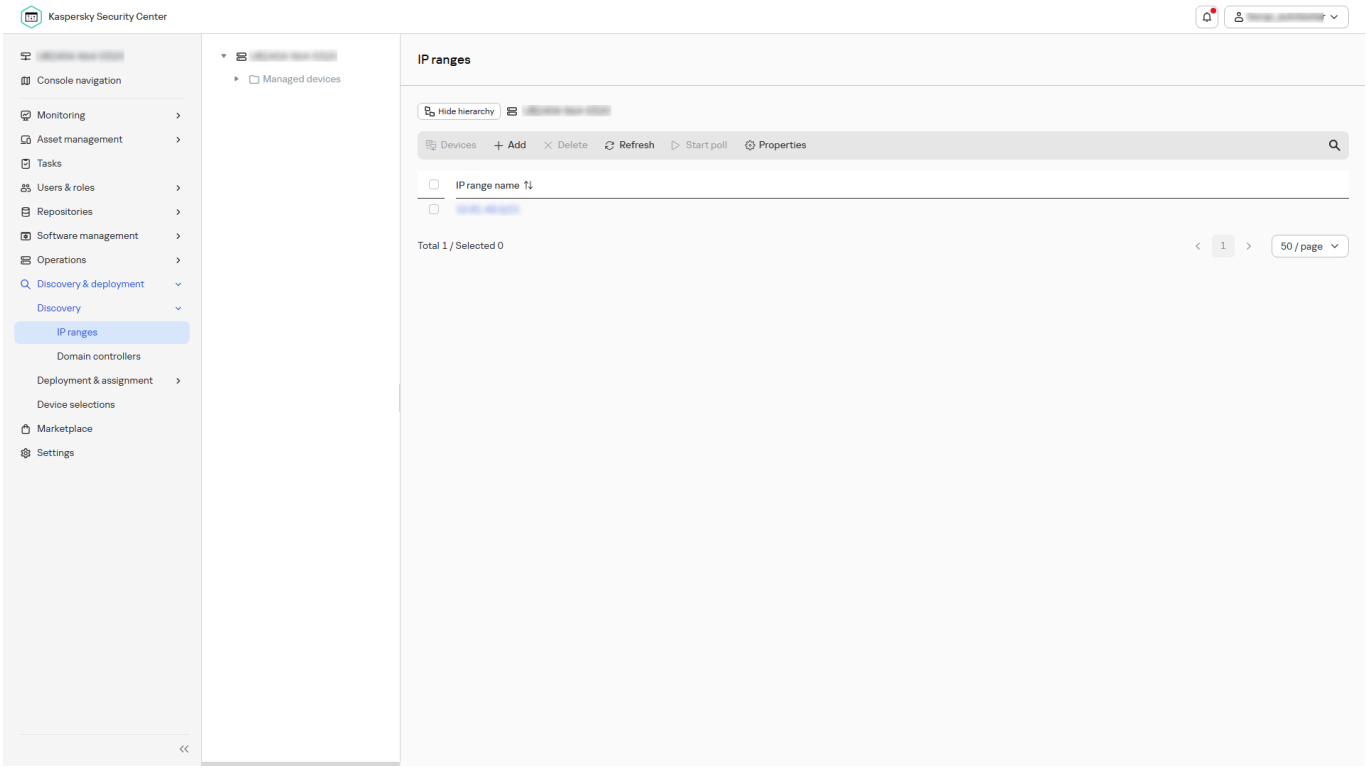
Если включен только опрос IP-диапазонов, Kaspersky Security Center Linux обнаруживает устройства только с IPv4-адресами. Если в вашей сети есть IPv6-устройства, включите опрос Zeroconf устройств.

Для всех устройств с операционной системой Linux в контроллере домена Microsoft Active Directory, Samba, FreeIPA или ALD Pro укажите `netbios name` и параметры `workgroup` в файле `/etc/samba/smb.conf`. Иначе результаты опроса могут содержать дублирующиеся устройства.

Просмотр и изменение параметров опроса IP-диапазонов

Чтобы просмотреть и изменить параметры опроса IP-диапазонов:

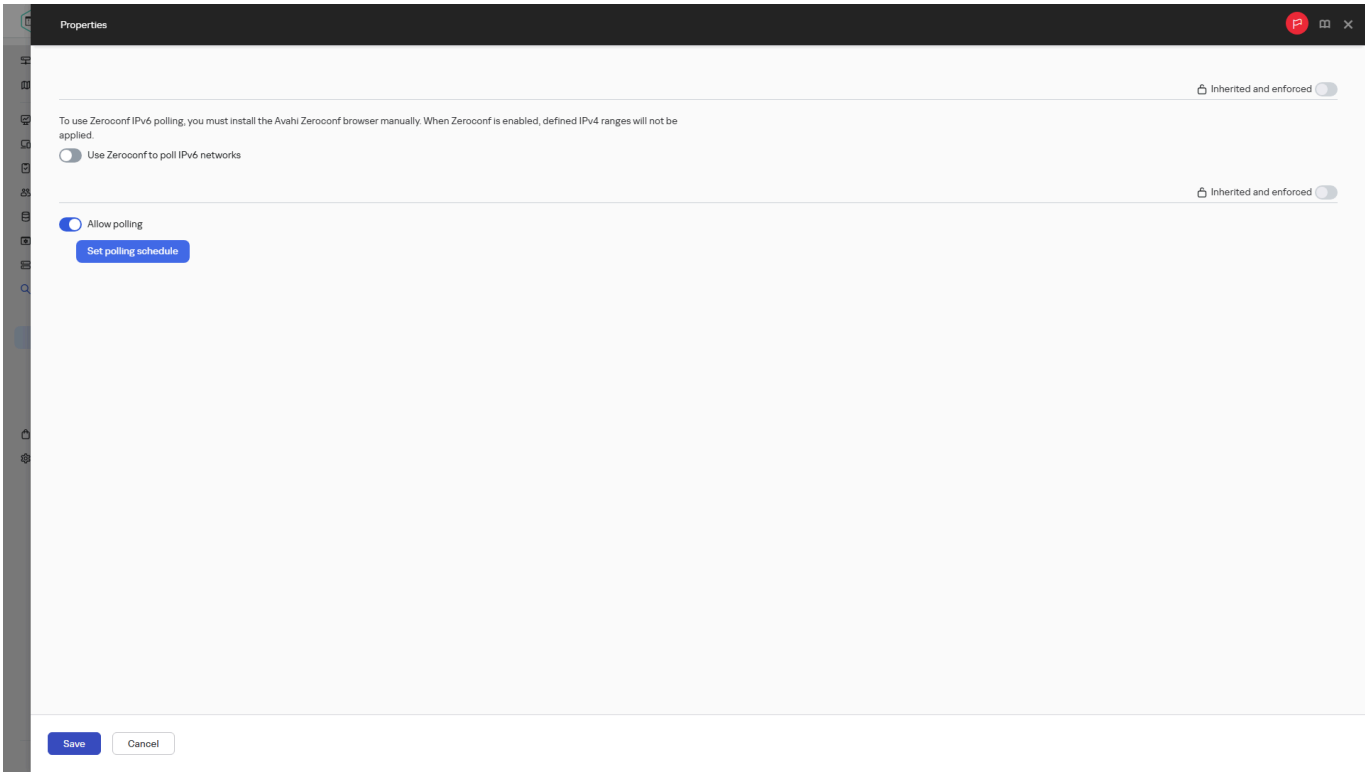
1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **IP-диапазоны**.



Список IP-диапазонов

2. Нажмите на кнопку **Свойства**.

Откроется окно свойств опроса IP-диапазонов.



Параметры 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 выбранный день**

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

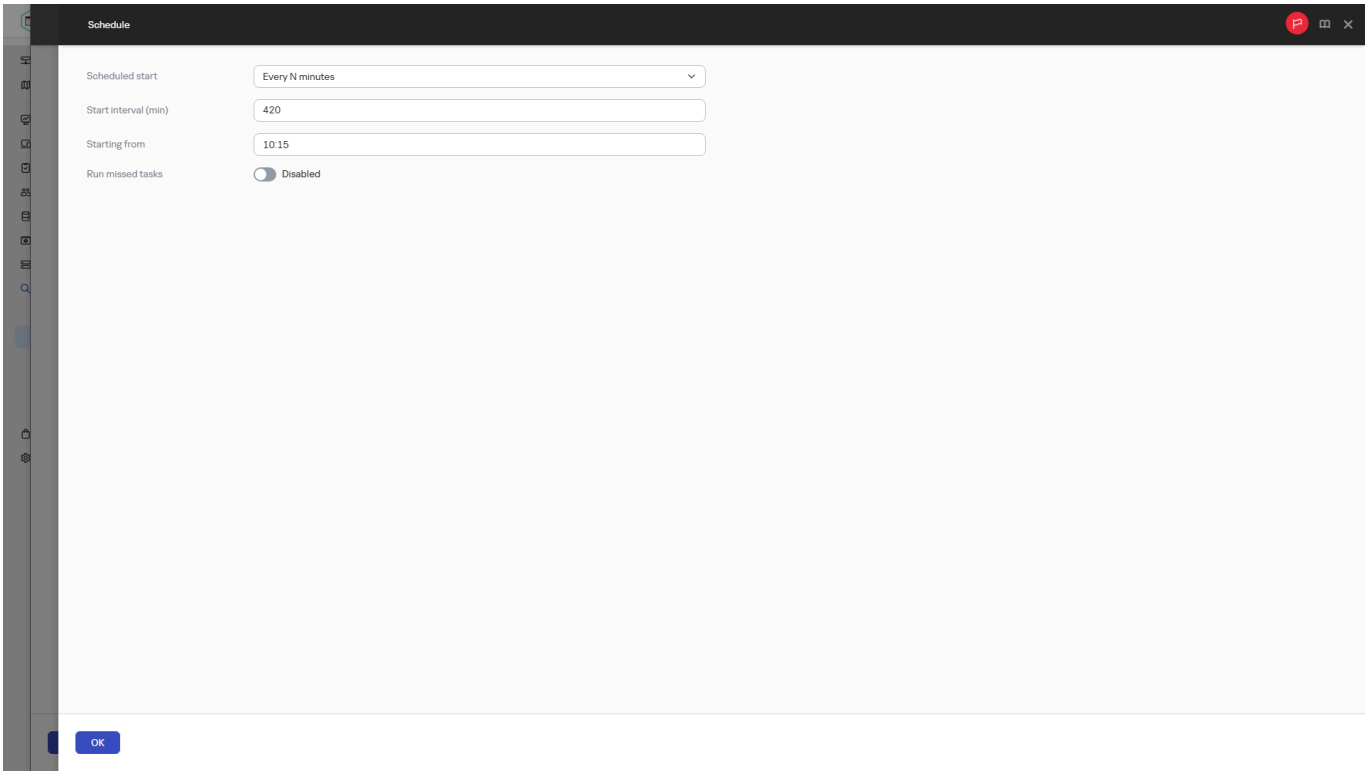
- **Запускать пропущенные задачи**

  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.



Настройка расписания опроса

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**.

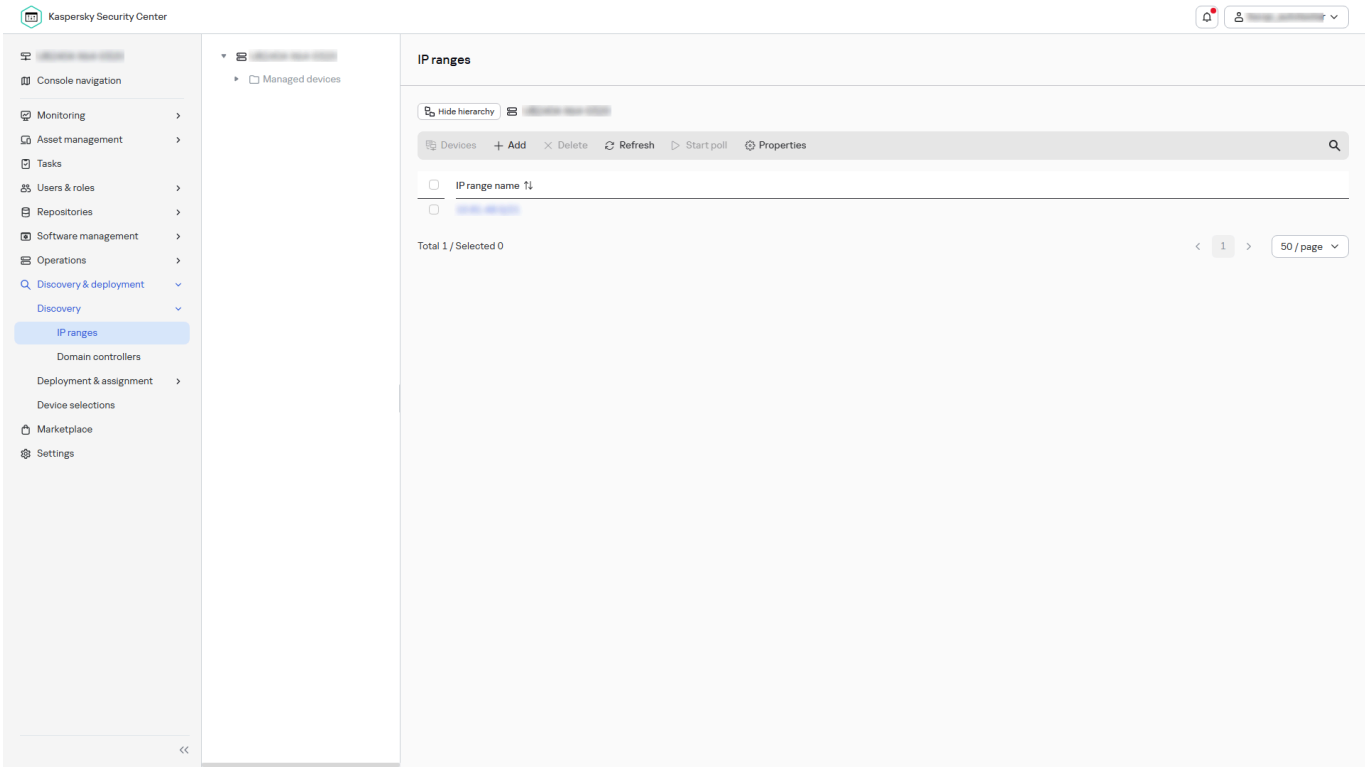
Добавление и изменение IP-диапазона

Исходно Kaspersky Security Center Linux 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 Linux автоматически включит сеть 192.168.0.0/24 в список адресов для опроса. Kaspersky Security Center Linux 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 Linux будет опрашивать всю сеть.

Чтобы добавить новый IP-диапазон:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание → Обнаружение устройств → IP-диапазоны**.



Список IP-диапазонов

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.

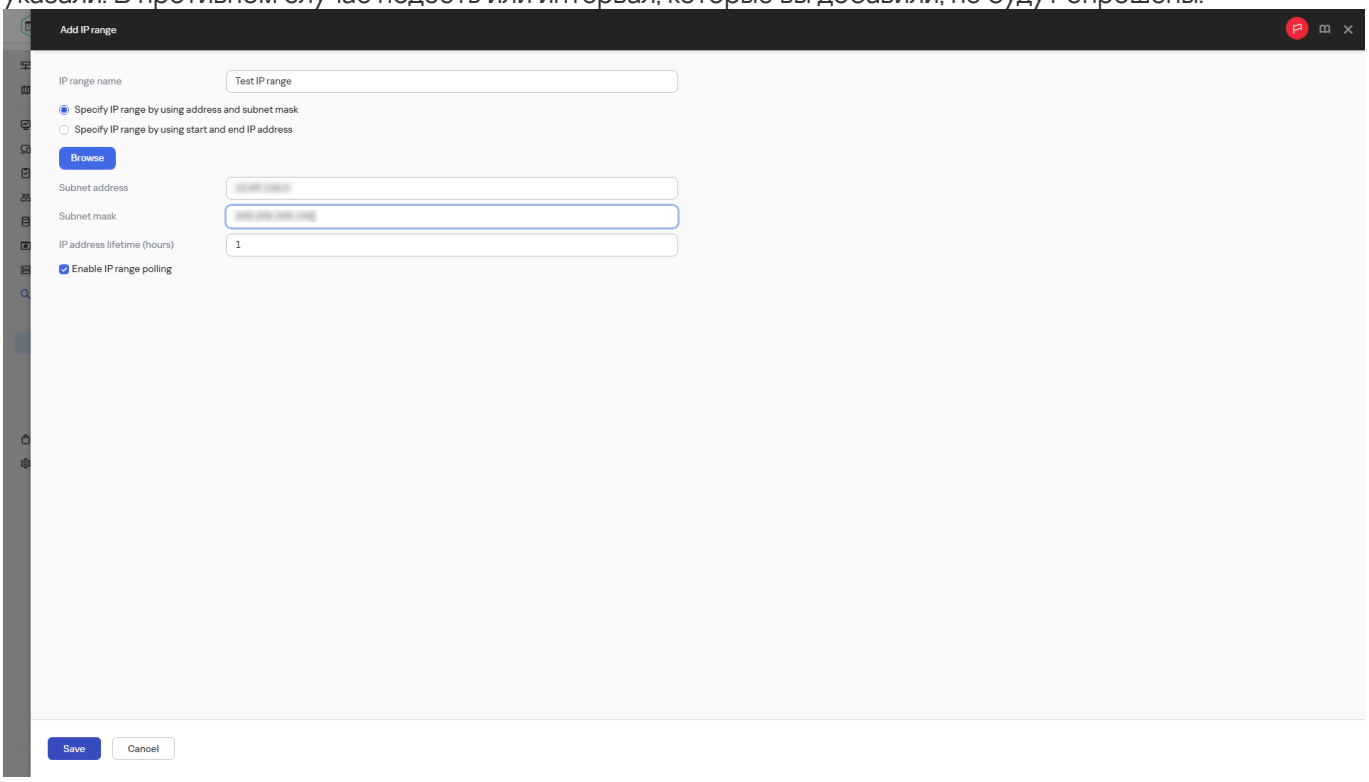
   IP-интервал или адрес и маска подсети

   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.



Указание параметров IP-диапазонов

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**. По умолчанию срок действия результатов опроса составляет 24 часа, он равен времени действия IP-адреса.

Чтобы добавить подсеть в существующий IP-диапазон:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **IP-диапазоны**.

2. Нажмите на имя IP-диапазона, в который вы хотите добавить подсеть.

3. В появившемся окне нажмите на кнопку **Добавить**.

4. Укажите подсеть либо с помощью ее адреса и маски, либо задав первый и последний IP-адреса в IP-диапазоне. Или добавить существующую подсеть, нажав на кнопку **Обзор**.

5. Нажмите на кнопку **Сохранить**.

   Подсеть добавлена в IP-диапазон.

6. Нажмите на кнопку **Сохранить**.

   Параметры IP-диапазона сохранены.

Вы можете добавить столько подсетей, сколько необходимо. Именованные IP-диапазоны не должны пересекаться, но на неименованные подсети внутри IP-диапазонов это ограничение не распространяется. Вы можете включить или отключить опрос независимо для каждого IP-диапазона.

Опрос Zeroconf

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

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

При использовании Zeroconf Сервер администрирования или точка распространения сканирует сеть для обнаружения устройств, поддерживающих протокол Zeroconf, и временно заносит их в список. Затем для каждого устройства выполняется ICMPv6-пинг для проверки доступности, а с помощью службы avahi производится обратный просмотр DNS для разрешения IPv6-адресов в DNS-имена. Информация о системе хоста (DNS-имя и тип ОС) регистрируется в базе данных Kaspersky Security Center Linux.

Область поиска устройств при опросе Zeroconf определяется настройками службы avahi. По умолчанию выполняется широковещательный опрос в рамках одной подсети. Если на устройстве с Сервером администрирования или точкой распространения настроено несколько сетевых интерфейсов, служба avahi опрашивает подсети, связанные со всеми активными интерфейсами.

Рекомендации для успешного выполнения опроса Zeroconf

- Убедитесь, что в файле /etc/avahi/avahi-daemon.conf установлены следующие значения для параметров:
  - На Сервере администрирования или точке распространения:
    `[server]`
    `use-ipv6=yes`
  - На устройствах:
    `[server]`
    `use-ipv6=yes`
    `[publish]`
    `publish-addresses=yes`
    `publish-workstation=yes`
- Убедитесь, что в файле /etc/nsswitch.conf присутствует следующая строка:
  - На Сервере администрирования или точке распространения:
    `mdns_minimal [NOTFOUND=return] dns`

Чтобы включить опрос Zeroconf:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **IP-диапазоны**.
2. Нажмите на кнопку **Свойства**.
3. В открывшемся окне включите переключатель **Использовать Zeroconf для опроса IPv6-сетей**.

После этого Kaspersky Security Center Linux начинает опрашивать вашу сеть. В этом случае указанные IP-диапазоны игнорируются.

Опрос контроллеров домена

Kaspersky Security Center Linux поддерживает опрос следующих типов контроллеров домена:

- Microsoft Active Directory.
- Samba.
- FreeIPA.
- ALD Pro.

Для контроллеров домена Samba, в качестве контроллеров домена Active Directory используется Samba 4.

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

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

Предварительные требования

Перед опросом контроллера домена убедитесь, что вы разрешаете подключения к контроллеру домена через сетевой экран или прокси-сервер. Также убедитесь, что на контроллере домена включены следующие протоколы:

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

  Этот протокол используется, если соединение с контроллером домена установлено с использованием SASL-аутентификации. Сервер администрирования и точки распространения поддерживают только механизм DIGEST-MD5.
- Lightweight Directory Access Protocol через Secure Sockets Layer (LDAPS)

  Этот протокол используется, если вам нужно подключиться к контроллеру домена по зашифрованному подключению.

Необходимо убедиться, что на устройстве контроллеров домена доступны следующие порты:

- 389 для LDAP-протокола и Simple Authentication (включая SASL).
- 636 для LDAPS-протокола.

Для FreeIPA и ALD Pro протоколы LDAP и LDAPS используются только для опроса домена. Kaspersky Security Center Linux не поддерживает аутентификацию учетных записей FreeIPA по LDAP(S). Чтобы разрешить пользователям FreeIPA и ALD Pro выполнять вход в Web Console, необходимо настроить аутентификацию Kerberos с помощью службы IAM.

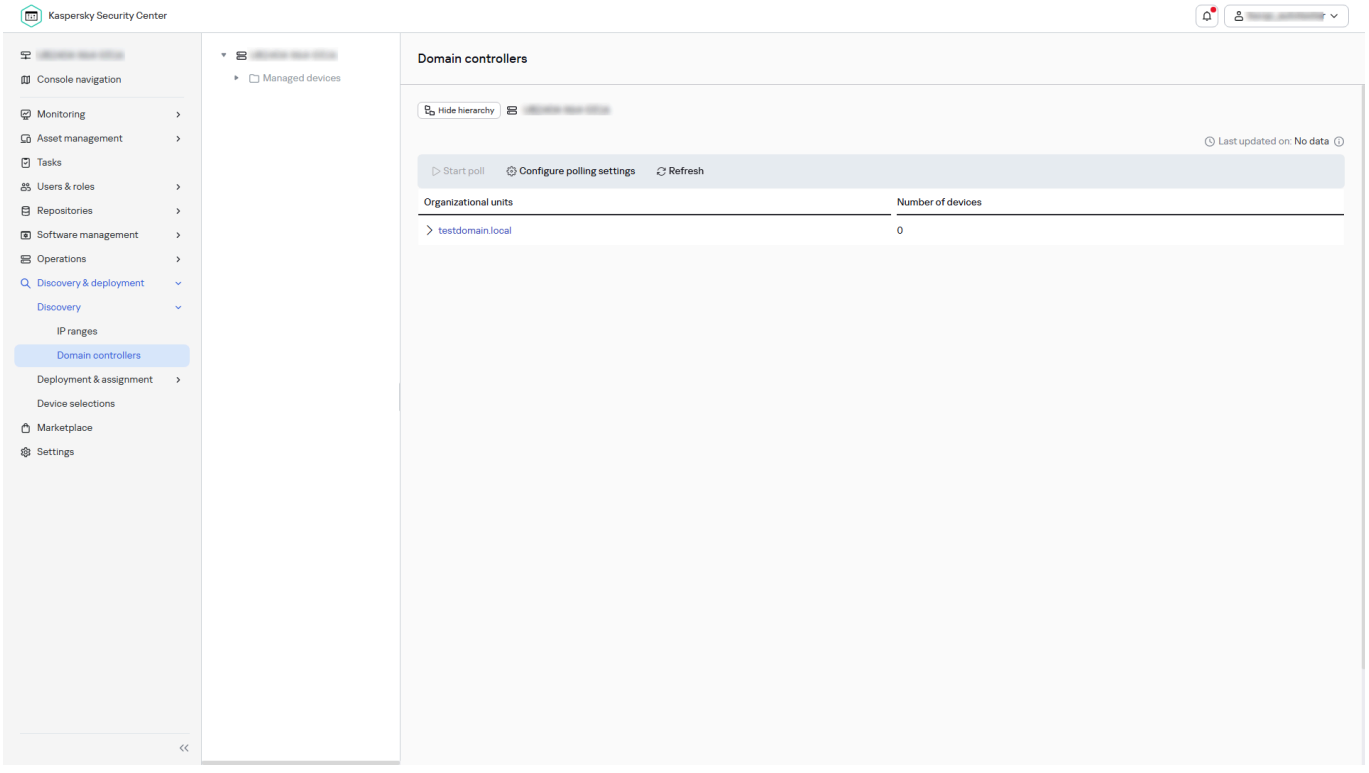
Для всех устройств с операционной системой Linux в контроллере домена Microsoft Active Directory, Samba, FreeIPA или ALD Pro вам нужно указать `netbios name` и параметры `workgroup` в файле `/etc/samba/smb.conf`. Иначе результаты опроса могут содержать дублирующиеся устройства.

Если домен Microsoft Active Directory содержит несколько контроллеров домена, выбор конкретного контроллера во время опроса домена не поддерживается. Соединение устанавливается с первым обнаруженным контроллером домена. Для обеспечения корректной аутентификации в домене Microsoft Active Directory поле альтернативного имени субъекта (SAN) сертификата должно включать все адреса контроллеров домена, входящих в этот домен, а также NetBIOS-имя домена Microsoft Active Directory.

Опрос контроллеров домена с помощью Сервера администрирования

Чтобы опросить контроллеры домена с помощью Сервера администрирования:

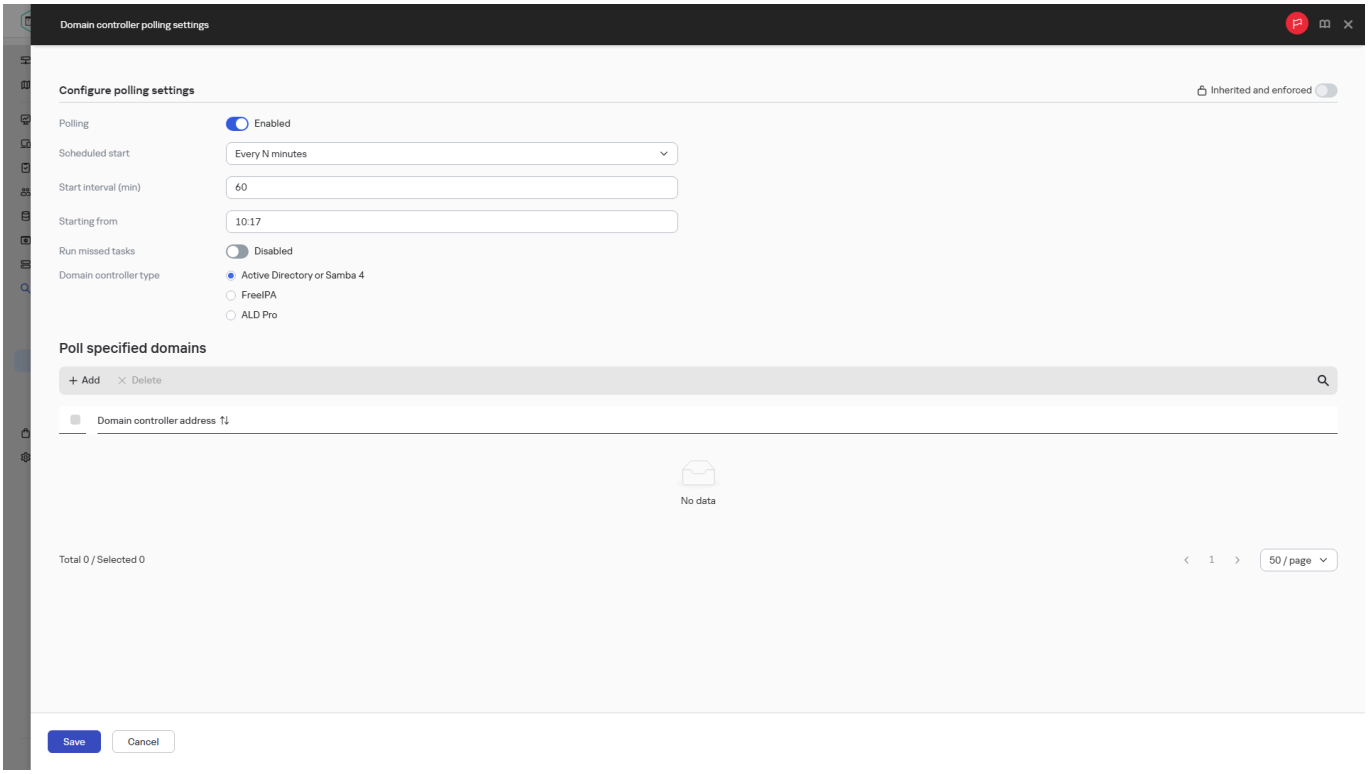
1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание → Обнаружение устройств → Контроллеры доменов**.



Окно опроса контроллеров домена

2. Нажмите на кнопку **Настроить параметры опроса**.

   Откроется окно **Параметры опроса контроллеров домена**.



Параметры опроса контроллеров домена

3. В поле **Опрос** установите переключатель в положение **Включено**.

4. В разделе **Опросить указанные домены** нажмите на кнопку **Добавить**, укажите адрес и учетные данные пользователя контроллеров домена.

5. В окне **Параметры опроса контроллеров домена** выполните следующие действия:

   - Выберите тип опроса контроллера домена: **Active Directory или Samba 4**, **FreeIPA**, **ALD Pro**.

   - При необходимости настройте расписание опроса. По умолчанию период опроса составляет один час. Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

     Доступны следующие варианты расписания опроса сети:

     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 выбранный день

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

     Запускать пропущенные задачи

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

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

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

По умолчанию параметр выключен.

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

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

Опрос контроллеров домена с помощью точки распространения

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

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

Чтобы настроить опрос контроллеров домена с помощью точки распространения:

1. Откройте свойства точки распространения.
2. Выберите раздел **Опрос контроллеров домена**.
3. В поле **Опрос** установите переключатель в положение **Включено**.
4. Если вы используете точку распространения с операционной системой Linux, выберите тип опроса контроллера домена: **Active Directory или Samba 4**, **FreeIPA**, **ALD Pro**.

   Необязательно указывать один и тот же тип контроллера домена при настройке опроса с помощью точки распространения и с помощью Сервера администрирования.
5. Выберите контроллеры домена, которые вы хотите опросить.

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

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

- **Опросить текущий домен**
- **Опросить весь лес доменов**
- **Опросить указанные домены**

6. Нажмите на кнопку **Настроить расписание опроса**, чтобы указать параметры расписания опроса при необходимости.

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

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

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

Обнаруженные учетные записи пользователей могут быть использованы для доменной аутентификации в Kaspersky Security Center Web Console.

Аутентификация и подключение к контроллеру домена

Аутентификация и подключение к контроллеру домена при опросе домена

При опросе контроллера домена Сервер администрирования или точка распространения определяет протокол соединения для установления начального соединения с контроллером домена. Этот протокол используется для всех будущих подключений к контроллеру домена. При первоначальном подключении к контроллеру домена вы можете изменить параметры подключения с помощью флагов Агента администрирования (`KLNAG_LDAP_TLS_REQCERT` и `KLNAG_LDAP_SSL_CACERT`). Вы можете настроить флаги Агента администрирования с помощью команды klscflag, как описано в этой статье.

Первоначальное подключение к контроллеру домена происходит следующим образом:

1. Сервер администрирования или точка распространения пытается подключиться к контроллеру домена через LDAPS.

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

   Возможные значения флага `KLNAG_LDAP_TLS_REQCERT`:

   - `0` – сертификат запрошен, но если он не предоставлен или проверка сертификата завершилась неудачно, соединение TLS по-прежнему считается успешно созданным (значение по умолчанию).
   - `1` – требуется строгая проверка сертификата LDAP-сервера.

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

2. В случае сбоя подключения LDAPS Сервер администрирования или точка распространения пытается подключиться к контроллеру домена по незашифрованному TCP-соединению с помощью SASL (DIGEST-MD5).

Аутентификация и подключение к контроллеру домена при аутентификации доменного пользователя на Сервере администрирования

Когда доменный пользователь выполняет аутентификацию на Сервере администрирования, Сервер администрирования определяет протокол для установки соединения с контроллером домена.

Для FreeIPA и ALD Pro протоколы LDAP и LDAPS используются только для опроса домена. Kaspersky Security Center Linux не поддерживает аутентификацию учетных записей FreeIPA по LDAP(S). Чтобы разрешить пользователям FreeIPA и ALD Pro выполнять вход в Web Console, необходимо настроить аутентификацию Kerberos с помощью службы IAM.

Подключение к контроллеру домена происходит следующим образом:

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

   Требуется строгая проверка сертификата LDAP-сервера.

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

2. В случае сбоя подключения LDAPS возникает ошибка подключения к контроллеру домена и другие протоколы подключения не используются.

Настройка флагов

Вы можете использовать утилиту klscflag для настройки флагов.

Запустите командную строку и измените текущую директорию на директорию с утилитой klscflag. На устройстве Сервера администрирования утилита klscflag находится в директории установки. По умолчанию задан путь /opt/kaspersky/ksc64/sbin.

Например, следующая команда принудительно проверяет сертификат:

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

Настройка доменной аутентификации для Сервера администрирования с помощью флагов

Поддерживается только Simple/SASL аутентификация (по паролю; SASL DIGEST-MD5; SASL EXTERNAL-TLS) на Сервере администрирования через Microsoft Active Directory.

Аутентификация FreeIPA/ALD Pro не поддерживается.

Чтобы выполнить доменную Simple/SASL аутентификацию:

1. На контроллере домена настройте протокол LDAPS (LDAP over TLS).

   Для этого получите, установите и настройте на контроллере домена корневой и/или промежуточный сертификат центра сертификации, выдавшего сертификат контроллеру, либо самоподписанный сертификат контроллера домена. Порядок настройки сертификата для LDAPS описан в документации Microsoft Active Directory.

2. В поле **SAN** сертификата укажите адреса всех контроллеров доменов и имя домена.

   При аутентификации Сервер администрирования выполнит строгую проверку сертификата контроллера домена.

3. Поместите сертификат контроллера домена в системное хранилище сертификатов.

   Если вы хотите хранить сертификат в отдельной директории, задайте путь к файлу сертификата LDAP-сервера с помощью флага KLNAG_LDAP_SSL_CACERT:

   ```
   klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v
   "/var/opt/kaspersky/ldap_cert.crt"
   ```

Сканирование домена выполнено.

Нажмите здесь, чтобы просмотреть примеры установки сертификата контроллера домена в системное хранилище сертификатов для различных операционных систем.

Для операционных систем Ubuntu/Debian

1. Если у вас не установлен пакет для работы с системным хранилищем сертификатов, установите его, выполнив команду:

   ```
   sudo apt-get install -y ca-certificates
   ```

2. Скопируйте файл с сертификатом в директорию /usr/local/share/ca-certificates sudo cp local-ca.crt, выполнив команду:

   ```
   sudo cp local-ca.crt /usr/local/share/ca-certificates
   ```

   где `local-ca.crt` – пример имени файла с сертификатом.

3. Добавьте сертификат в системное хранилище, выполнив команду:

   ```
   sudo cp local-ca.crt /usr/local/share/ca-certificates
   ```

Для операционной системы CentOS

1. Если у вас не установлен пакет для работы с системным хранилищем сертификатов, установите его, выполнив команду:

   ```
   sudo yum install -y ca-certificates
   ```

2. Если вы используете CentOS версии 7 и ниже, выполните команду:

   ```
   sudo update-ca-trust force-enable
   ```

3. Скопируйте файл с сертификатом в директорию /etc/pki/ca-trust/source/anchors/, выполнив команду:

   ```
   sudo cp local-ca.crt /etc/pki/ca-trust/source/anchors/
   ```

   где `local-ca.crt` – пример имени файла с сертификатом.

4. Добавьте сертификат в системное хранилище, выполнив команду:

   ```
   sudo update-ca-trust
   ```

Настройка доменной Simple/SASL аутентификации выполняется с помощью следующих флагов:

- `KLNAG_LDAP_REFERRAL_BEHAVIOR` – управляет обработкой реферального ответа при поиске пользователя на контроллере домена, который используется для аутентификации.

  Значение по умолчанию: `KLNAG_LDAP_REFERRAL_BEHAVIOR = 1`

- `KLNAG_LDAP_USR_INFO_IGNORE_REF_ERR` – управляет обработкой реферального ответа при запросе дополнительных данных этого пользователя.

  Значение по умолчанию: `KLNAG_LDAP_USR_INFO_IGNORE_REF_ERR = 0`

Рекомендуется оставлять значения флагов по умолчанию, за исключением следующих случаев:

- В вашей инфраструктуре несколько контроллеров домена и/или несколько доменных зон, а учетная запись, используемая для аутентификации на Сервере администрирования, может находиться на разных контроллерах домена и иметь отличающийся SID. При этом реферальные ответы (LDAP referral) от глобального каталога не приводят к недоступным контроллерам.

  Для флага `KLNAG_LDAP_REFERRAL_BEHAVIOR` установите значение `2`, выполнив команду:

  ```
  ./klscflag -fset -pv klnagent -n KLNAG_LDAP_REFERRAL_BEHAVIOR -t d -v 2
  ```

- В вашей инфраструктуре возможны реферальные ответы, указывающие на недоступные контроллеры домена (например, из-за сетевых ограничений).

  Установите значения флагов `KLNAG_LDAP_REFERRAL_BEHAVIOR=0` и `KLNAG_LDAP_USR_INFO_IGNORE_REF_ERR=1`, выполнив команды:

  ```
  ./klscflag -fset -pv klnagent -n KLNAG_LDAP_REFERRAL_BEHAVIOR -t d -v 0
  ./klscflag -fset -pv klnagent -n KLNAG_LDAP_USR_INFO_IGNORE_REF_ERR -t d -v 1
  ```

Настройка контроллеров домена Samba

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

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

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

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

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

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

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

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

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

Для всех устройств с операционной системой Linux в контроллере домена Samba в файле `/etc/samba/smb.conf` нужно указать `netbios name` и параметры `workgroup`. Иначе результаты опроса могут содержать дублирующиеся устройства.

Инвентаризация оборудования

В списке оборудования (**Управление активами** → **Оборудование**), который вы используете для инвентаризации оборудования, заполняется двумя способами: автоматически и вручную. После каждого опроса сети все обнаруженные устройства автоматически добавляются в список; однако вы также можете добавить устройства вручную, если не хотите опрашивать сеть. Вы можете добавить другие устройства в список вручную, например, маршрутизаторы, принтеры или оборудование.

В свойствах устройства можно просматривать и редактировать подробную информацию об устройствах.

В списке оборудования могут присутствовать следующие типы устройств:

- компьютеры;
- мобильные устройства;
- сетевые устройства;
- виртуальные устройства;
- компьютерные комплектующие;
- компьютерная периферия;
- подключаемые устройства;

- VoIP-телефоны;
- сетевые хранилища.

Администратор может присваивать обнаруженным устройствам признак *Корпоративное оборудование*. Этот признак можно присвоить в свойствах устройства вручную или задать критерии для его автоматического присвоения. В этом случае признак *Корпоративное оборудование* присваивается по типу устройства.

Kaspersky Security Center Linux позволяет выполнять списание оборудования. Для этого в свойствах устройства необходимо выбрать параметр **Списано**. Такое устройство не отображается в списке оборудования.

Администратор может работать со списком программируемых логических контроллеров (ПЛК) в папке **Оборудование**. Подробная информация о работе со списками ПЛК приведена в *Руководстве пользователя Kaspersky Industrial CyberSecurity for Nodes*.

Добавление информации о новых устройствах

Чтобы добавить информацию о новых устройствах в сети:

1. В главном окне приложения перейдите в раздел **Управление активами → Оборудование**.
2. Нажмите на кнопку **Добавить**, чтобы открыть окно **Новое устройство**.
3. В окне **Новое устройство** в раскрывающемся списке **Тип устройства** выберите тип устройства, которое вы хотите добавить.
4. Нажмите на кнопку **ОК**.

   Откроется окно свойств устройства на разделе **Общие**.
5. В разделе **Общие** заполните поля ввода данными об устройстве. В разделе **Общие** доступны следующие параметры:
   - **Корпоративное устройство**. Установите флажок, если вы хотите присвоить устройству признак *Корпоративное*. По этому признаку можно выполнять поиск устройств в папке **Оборудование**.
   - **Списано**. Установите флажок, если вы не хотите, чтобы устройство отображалось в списке устройств в папке **Оборудование**.
6. Нажмите на кнопку **Применить**.

Новое устройство отобразится в рабочей области страницы **Оборудование**.

Настройка критериев определения корпоративных устройств

Чтобы настроить критерии определения корпоративных устройств:

1. В главном окне приложения перейдите в раздел **Управление активами → Оборудование**.
2. В верхней части страницы **Оборудование** нажмите на ссылку **Настроить критерии определения корпоративных устройств**.

   Откроется панель **Настроить критерии определения корпоративных устройств**.
3. В панели **Настроить критерии определения корпоративных устройств** включите параметр **Автоматически устанавливать для устройства признак "Корпоративное"**. Укажите типы устройств, которым атрибут *Корпоративное* назначается автоматически.

   Этот параметр влияет только на те устройства, которые были добавлены с помощью опроса сети. Для устройств, добавленных вручную, установите параметр *Корпоративное* вручную.
4. Нажмите на кнопку **OK**.

Критерии обнаружения корпоративных устройств настроены.

Использование динамического режима VDI на клиентских устройствах

В сети организации может быть развернута виртуальная инфраструктура с использованием временных виртуальных машин. Kaspersky Security Center Linux обнаруживает временные виртуальные машины и добавляет информацию о них в базу данных Сервера администрирования. После завершения работы пользователя с временной виртуальной машиной машина удаляется из виртуальной инфраструктуры. Однако запись об удаленной виртуальной машине может сохраниться в базе данных Сервера администрирования. Также несуществующие виртуальные машины могут отображаться в Kaspersky Security Center Web Console.

Чтобы избежать сохранения данных о несуществующих виртуальных машинах, в Kaspersky Security Center Linux реализована поддержка динамического режима для Virtual Desktop Infrastructure (VDI). Администратор может включить поддержку динамического режима для VDI в свойствах инсталляционного пакета Агента администрирования, который будет установлен на временной виртуальной машине.

Во время выключения временной виртуальной машины Агент администрирования информирует Сервер администрирования о выключении. В случае успешного выключения виртуальной машины, она удаляется из списка устройств, подключенных к Серверу администрирования. Если выключение виртуальной машины выполнено некорректно и Агент администрирования не послал Серверу уведомление о выключении, используется дублирующий сценарий. Согласно этому сценарию виртуальная машина удаляется из списка устройств, подключенных к Серверу администрирования, после трех неудачных попыток синхронизации с Сервером.

Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования

Чтобы включить динамический режим VDI:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета Агента администрирования выберите пункт **Свойства**.

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

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

Перемещение в группу администрирования устройств, являющихся частью VDI

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

1. Перейдите в раздел **Управление активами** → **Правила перемещения**.
2. Нажмите на кнопку **Добавить**.
3. На вкладке **Условия правила** выберите вкладку **Виртуальные машины**.
4. Установите для правила **Является виртуальной машиной** значение **Да** и для **Часть Virtual Desktop Infrastructure** значение **Да.**
5. Нажмите на кнопку **Сохранить**.

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

Чтобы просмотреть параметры управляемого устройства:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.

   Отобразится список управляемых устройств.

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

Откроется окно свойств выбранного устройства.

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

Общие

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.

- **Статус устройства**

  Статус клиентского устройства, формируемый на основании установленных администратором критериев состояния антивирусной защиты на устройстве и активности устройства в сети.

- **Полное название группы**

  Группа администрирования, в состав которой входит клиентское устройство.

- **Последнее обновление антивирусных баз**

  Дата последнего обновления антивирусных баз или приложений на устройстве.

- **Соединение с Сервером администрирования**

  Дата и время последнего соединения Агента администрирования, установленного на клиентском устройстве, с Сервером администрирования.

- **Последнее появление в сети**

  Дата и время, когда устройство последний раз было видимо в сети.

- **Версия Агента администрирования**

  Версия установленного Агента администрирования.

- **Создано**

  Дата создания устройства в Kaspersky Security Center Linux.

- **Владелец устройства**

  Имя владельца устройства. Вы можете назначить или удалить пользователя в качестве владельца устройства, нажав на ссылку **Сменить владельца устройства**.

- **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.

- **IPv6-адрес**

- В разделе **Система** представлена информация об операционной системе, установленной на клиентском устройстве:

  - **ОС**

  - **Архитектура процессора**

  - **Имя устройства**

  - **Тип виртуальной машины**

    Производитель виртуальной машины

  - **Динамическая виртуальная машина как часть VDI**

    В этой строке показано, является ли клиентское устройство динамической виртуальной машиной как часть VDI.

- В разделе **Защита** представлена следующая информация о состоянии антивирусной защиты на клиентском устройстве:

  - **Видимо в сети**

    Статус видимости клиентского устройства.

  - **Статус устройства**

    Статус клиентского устройства, формируемый на основании установленных администратором критериев состояния антивирусной защиты на устройстве и активности устройства в сети.

  - **Описание статуса**

    Статус защиты клиентского устройства и подключения к Серверу администрирования.

  - **Состояние защиты**

    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 полная проверка**

    Дата и время последнего поиска вредоносного ПО на клиентском устройстве.

- **Обнаружен вирус**

  Общее количество обнаруженных на клиентском устройстве угроз с момента установки приложения безопасности (первой проверки устройства) либо с момента последнего обнуления счетчика угроз.

- **Объекты, которые не удалось вылечить**

  Количество необработанных файлов на клиентском устройстве.

  В поле не учитывается количество необработанных файлов для мобильных устройств.

- **Статус шифрования дисков**

  Текущее состояние шифрования файлов на локальных дисках устройства. Описание статусов см. в онлайн-справке Kaspersky Endpoint Security для Windows.

  Файлы могут быть зашифрованы только на управляемых устройствах, на которых установлен Kaspersky Endpoint Security для Windows.

- В разделе **Статус устройства определен приложением** отображается информация о статусе устройства, который определен управляемым приложением, установленным на клиентском устройстве. Это состояние устройства может отличаться от того, которое определено Kaspersky Security Center Linux.

Приложения

На этой вкладке отображается список приложений "Лаборатории Касперского", установленных на клиентском устройстве. На этой вкладке находятся кнопки **Запустить** и **Остановить**, которые позволяют запускать и останавливать выбранное приложение "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 приложение появится сообщение об ошибке. Также вы можете нажать на имя приложения, чтобы просмотреть общую информацию о приложении, список событий, произошедших на устройстве, и параметры приложения.

Действующие политики и профили политик

На этой вкладке отображаются списки политик и профилей политик, которые назначены управляемому устройству.

Задачи

На вкладке **Задачи** вы можете управлять задачами клиентского устройства: просматривать список существующих задач, создавать новые, удалять, запускать и останавливать задачи, изменять их параметры и просматривать результаты выполнения. Список задач предоставляется на основании данных, полученных в ходе последней синхронизации клиента с Сервером администрирования. Информация о статусе задач запрашивается Сервером администрирования с клиентского устройства. 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 push-сервер не может получить доступ к управляемому устройству, но включен режим постоянного подключения к Серверу администрирования (параметр **Не разрывать соединение с Сервером администрирования** с Сервером администрирования в разделе **Общие** включен), действия с задачами доступны.

В случае отсутствия связи статус не отображается и кнопки неактивны.

События

На вкладке **События** отображаются события, зарегистрированные на Сервере администрирования для выбранного клиентского устройства.

Вы можете экспортировать, копировать и удалять события устройства.

Проблемы безопасности

На вкладке **Проблемы безопасности** можно просматривать, изменять и создавать проблемы безопасности для клиентского устройства. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором. Например, если пользователь постоянно переносит на устройство вредоносные приложения с личного съемного диска, администратор может создать проблему безопасности. Администратор может указать краткое описание случая и рекомендуемых действий (таких как дисциплинарные действия), которые должны быть предприняты против пользователя в тексте проблемы безопасности, и может добавить ссылку на пользователя или пользователей.

Проблема безопасности, для которой выполнены необходимые действия, называется *обработанным*. Наличие необработанных проблем безопасности может быть выбрано условием для изменения статуса устройства на *Критический* или *Предупреждение*.

В разделе содержится список проблем безопасности, созданных для устройства. Проблемы безопасности классифицируются по уровню важности и типу. Тип проблемы безопасности определяется приложением "Лаборатории Касперского", которое создает проблему безопасности. Обработанные проблемы безопасности можно отметить в списке, установив флажок в столбце **Обработана**.

Теги

На вкладке **Теги** можно управлять списком ключевых слов, на основании которых выполняется поиск клиентского устройства: просматривать список существующих тегов, назначать теги из списка, настраивать правила автоматического назначения тегов, добавлять новые теги и переименовывать старые теги, удалять теги.

Дополнительно

Эта вкладка содержит следующие разделы:

- **Реестр приложений**. В этом разделе можно просмотреть реестр установленных на клиентском устройстве приложений и обновлений для них, а также настроить отображение реестра приложений.

  Информация об установленных приложениях 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 приложения открывается окно, содержащее сведения о приложении и список пакетов обновлений, установленных для этого приложения.

- **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 приложение 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.

  Если Агент администрирования установлен на устройстве с операционной системой Windows, он отправляет на Сервер администрирования следующую информацию об аппаратном обеспечении устройства:

  - оперативная память;
  - запоминающие устройства;
  - материнская плата;
  - процессор;
  - сетевой адаптер;
  - мониторы;
  - видеоадаптер;
  - звуковая плата.

  Если Агент администрирования установлен на устройстве с операционной системой Linux или macOS, он отправляет на Сервер администрирования следующую информацию об аппаратном обеспечении устройства, если эта информация предоставляется операционной системой:

  - общий объем оперативной памяти;
  - общий объем запоминающих устройств;
  - материнская плата;
  - процессор;
  - сетевой адаптер.

- **Применимые обновления**. В этом разделе можно просмотреть список обнаруженных на устройстве обновлений программного обеспечения, которые не были установлены.

- **Уязвимости в приложениях**. В этом разделе можно просмотреть список с информацией об уязвимостях сторонних приложений, установленных на клиентских устройствах.

  Чтобы сохранить уязвимости в файл, установите флажки рядом с уязвимостями, которые вы хотите сохранить, и нажмите на кнопку **Экспортировать в CSV** или на кнопку **Экспортировать в TXT**.

  Раздел содержит следующие параметры:

  - **Показывать только те уязвимости, которые можно закрыть**

    Если параметр включен, в разделе отображаются уязвимости, которые можно закрыть патчем.

    Если параметр выключен, в разделе отображаются и уязвимости, которые можно закрыть патчем, и уязвимости, для которых патч отсутствует.

    По умолчанию параметр включен.

- **Свойства уязвимости**

  Нажмите на имя уязвимости в приложениях в списке, чтобы просмотреть свойства выбранной уязвимости в приложениях в отдельном окне. В окне свойств можно выполнить следующие действия:

  - Пропустить уязвимость в приложениях на этом управляемом устройстве (в Kaspersky Security Center Web Console).
  - Просмотреть список рекомендуемых исправлений для уязвимости.
  - Вручную указать обновления программного обеспечения для закрытия уязвимости (в Kaspersky Security Center Web Console).
  - Просмотреть экземпляр уязвимости.
  - Просмотреть список существующих задач для закрытия уязвимости и создать задачи для закрытия уязвимости.

- **Удаленная диагностика**. В этом разделе можно выполнять удаленную диагностику клиентских устройств.

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.

Проверка соединения клиентского устройства с Сервером администрирования вручную Утилита klnagchk

Вы можете проверять соединение и получать подробную информацию о параметрах подключения клиентского устройства к Серверу администрирования с помощью утилиты klnagchk. Утилита klnagchk находится в папке установки Агента администрирования.

При запуске из командной строки утилита klnagchk в зависимости от используемых ключей выполняет следующие действия:

- Выводит на экран или заносит в файл журнала событий значения параметров подключения Агента администрирования, установленного на устройстве, к Серверу администрирования.
- Записывает в файл журнала событий статистику Агента администрирования (с момента его последнего запуска) и результаты выполнения утилиты либо выводит информацию на экран.
- Пытается установить соединение Агента администрирования с Сервером администрирования.

  Если соединение установить не удалось, утилита посылает ICMP-пакет для проверки статуса устройства, на котором установлен Сервер администрирования.

Чтобы проверить соединение клиентского устройства с Сервером администрирования с помощью утилиты klnagchk,

на устройстве с установленным Агентом администрирования запустите утилиту klnagchk из командной строки под учетной записью локального администратора.

Синтаксис командной строки утилиты:

```
klnagchk [-logfile <имя файла>] [-sp] [-savecert <путь к файлу сертификата>] [-
restart][-sendhb]
```

Описания ключей:

- `-logfile <имя файла>` – записывает значения параметров подключения Агента администрирования к Серверу и результаты выполнения утилиты в файл журнала.

  По умолчанию информация сохраняется в стандартном потоке вывода (stdout). Если ключ не используется, параметры, результаты и сообщения об ошибках выводятся на экран.

- `-sp` – выводит пароль для аутентификации пользователя на прокси-сервере.

  Ключ используется, если подключение к Серверу администрирования осуществляется через прокси-сервер.

- `-savecert <имя файла>` – сохраняет сертификат для аутентификации доступа к Серверу администрирования в указанном файле.

- `-restart` – запускает Агент администрирования после завершения работы утилиты.

- `-sendhb` – запускает синхронизацию Агента администрирования с Сервером администрирования.

После запуска утилита klnagchk обращается к конфигурационным файлам Агента администрирования и отображает параметры подключения. Эти параметры задаются при установке Агента администрирования и в параметрах политики Агента администрирования:

- `Current device` – имя клиентского устройства в сети Windows.

- `Network Agent version` – номер версии Агента администрирования (с патчами), установленного на устройстве.

- `Server address` – адрес Сервера администрирования.

- `Use SSL` – параметр, указывающий, используется ли защищенное соединение при подключении к Серверу администрирования.

  Возможные значения:

  - 0 – защищенный канал не используется.

  - 1 – используется защищенный канал.

- `Compress traffic` – параметр, указывающий, сжимается ли трафик между клиентским устройством и Сервером администрирования.

- `Server SSL ports` – номера допустимых портов для подключения к Серверу администрирования при использовании защищенного канала.

- `Server ports` – номера портов, допустимых для подключения к Серверу администрирования при использовании обычного соединения.
- `Use proxy server` – параметр, указывающий, используется ли прокси-сервер.

  Возможные значения:

  - 0 – прокси-сервер не используется.
  - 1 – прокси-сервер используется.
- `Address` – адрес и порт прокси-сервера, разделенные двоеточием. Этот параметр отображается, только если используется прокси-сервер.
- `User name` – имя пользователя для доступа к прокси-серверу. Этот параметр отображается, только если используется прокси-сервер.
- `Password` – пароль для доступа к прокси-серверу. Этот параметр отображается, только если используется прокси-сервер. Чтобы показать пароль прокси-сервера, вам нужно использовать в команде ключ `sp`.
- `Certificate` – параметр, указывающий, есть ли у клиентского устройства сертификат Сервера администрирования. Сертификат может не существовать, например, если Агент администрирования ни разу не подключился к Серверу администрирования.

  Возможные значения:

  - `not installed` – на клиентском устройстве отсутствует сертификат Сервера администрирования.
  - `present` – клиентское устройство имеет сертификат Сервера администрирования.
- `Open UDP port` – параметр, указывающий, использует ли Агент администрирования UDP-порт для получения запросов на синхронизацию от Сервера администрирования.

  Возможные значения:

  - 0 – UDP-порт закрыт для приема запросов на синхронизацию от Сервера администрирования.
  - 1 – UDP-порт открыт для приема запросов на синхронизацию от Сервера администрирования.
- `UDP ports` – номера UDP-портов, которые может использовать Агент администрирования.
- `Location name` – сетевое местоположение устройства.
- `State of network location` – параметр, указывающий, можно ли переключить клиентское устройство с одного профиля соединений Сервера администрирования на другой.

  Возможные значения:

  - `Enabled` – профиль соединений к Серверу администрирования можно переключить для клиентского устройства.
  - `Disabled` – профиль соединений к Серверу администрирования переключить для клиентского устройства невозможно.
- `Profile to use` – профиль соединений к Серверу администрирования.
- `Condition` – IP-адрес и маска подсети сети, к которой подключено клиентское устройство.

- `Ping period, minutes` – стандартный интервал синхронизации.
- `Conn timeout, s` – время ожидания соединения.
- `RW timeout, s` – время ожидания соединения для операций чтения-записи.
- `Host ID` – идентификатор устройства в сети. `Device ID` уникален для клиентских устройств, управляемых определенным Сервером администрирования.
- `Locations of connection gateways` – параметры подключения клиентского устройства к Серверу администрирования с помощью шлюза соединения.
- `Location of distribution points` – параметры подключения клиентского устройства к Серверу администрирования с помощью точки распространения.
- `Connection with server` – параметр, указывающий, имеет ли шлюз соединения постоянное соединение с Сервером администрирования. Параметр отображается только в том случае, если клиентское устройство выступает в роли шлюза соединения.

  Возможные значения:

  - `active` – шлюз соединения имеет постоянное соединение с Сервером администрирования.
  - `inactive` – шлюз соединения не имеет постоянного соединения с Сервером администрирования.
- `Connection with server through connection gateway` – параметр, указывающий, правильно ли установлено соединение с Сервером администрирования с помощью шлюза соединения. Параметр отображается только в том случае, если клиентское устройство выступает в роли шлюза соединения.

  Возможные значения:

  - `active` – соединение с Сервером администрирования с помощью шлюза соединения установлено правильно.
  - `inactive` – соединение с Сервером администрирования с помощью шлюза соединения установлено некорректно.

Также вывод утилиты klnagchk может содержать одну из следующих строк:

- `Administration Server is installed on this device` – на устройстве Сервера администрирования запущена утилита klnagchk.
- `This device has been assigned a connection gateway but is not yet registered on Administration Server` – утилита klnagchk запущена на устройстве, на котором установлен Агент администрирования, выполняющий роль шлюза соединения. Настроенный шлюз соединения ожидает соединения от Сервера администрирования, но Сервер администрирования не перечисляет устройство среди управляемых устройств. Вам потребуется убедиться, что Сервер администрирования инициировал соединение со шлюзом соединения.
- `This device is a connection gateway` – утилита klnagchk запускается на устройстве, которое выполняет роль шлюза соединения.
- `Acts as a distribution point` – утилита klnagchk запускается на устройстве, которое выполняет роль точки распространения.

Утилита klnagchk проверяет состояние службы Агента администрирования. Если служба не запущена, утилита останавливается. Если служба запущена, утилита отображает следующую статистику подключений:

- `Ping count` – количество попыток подключения клиентского устройства к Серверу администрирования.
- `Succ. pings` – количество успешных попыток подключения клиентского устройства к Серверу администрирования.
- `Sync count` – количество попыток синхронизации параметров клиентского устройства с параметрами Сервера администрирования.
- `Succ. syncs` – количество успешных попыток синхронизации параметров клиентского устройства с Сервером администрирования.
- `Last ping` – дата и время последнего подключения.

При анализе соединения между Сервером администрирования и Агентом администрирования необходимо использовать параметры `Ping count` и `Succ. pings`. Параметры клиентского устройства синхронизируются с параметрами Сервера администрирования только в случае изменения параметров Сервера администрирования (например, при добавлении новых задач или изменении параметров политики). Иначе значения параметров `Ping count` и `Succ. pings` не изменяются.

Подробнее об устранении проблем с подключением Агента администрирования к Серверу администрирования см. Kaspersky Security Center Linux FAQ.

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 **Управление активами → Правила перемещения**.

Правило перемещения по умолчанию предназначено для однократного первоначального размещения устройств в группах администрирования. Правило перемещает нераспределенные устройства только один раз. 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 приложения* или создании автономного инсталляционного пакета.

Можно создать правило перемещения, способное многократно действовать на одно и то же устройство.

Настоятельно рекомендуется избегать подхода к работе с управляемыми устройствами, при котором одно и то же устройство многократно перемещается из группы в группу, например, с целью применения к устройству особой политики, запуска специальной групповой задачи, обновления с определенной точки распространения.

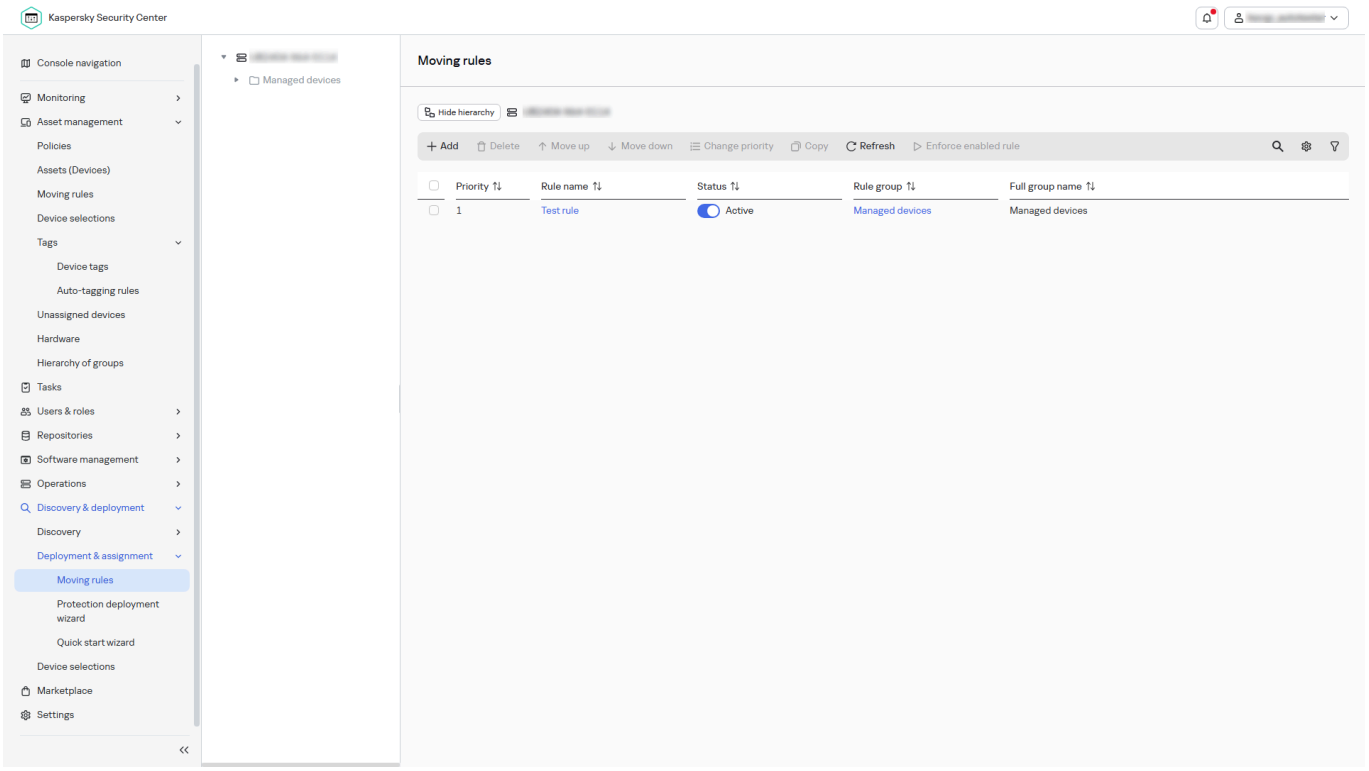
Подобные сценарии не поддерживаются, так как они крайне неэффективны по нагрузке на Сервер администрирования и на сетевой трафик. Также эти сценарии противоречат модели работы Kaspersky Security Center Linux (особенно в области прав доступа, событий и отчетов). Следует искать другое решение, например, использовать профили политик, задачи для выборок устройств, назначать Агенты администрирования согласно методике.

Создание правил перемещения устройств

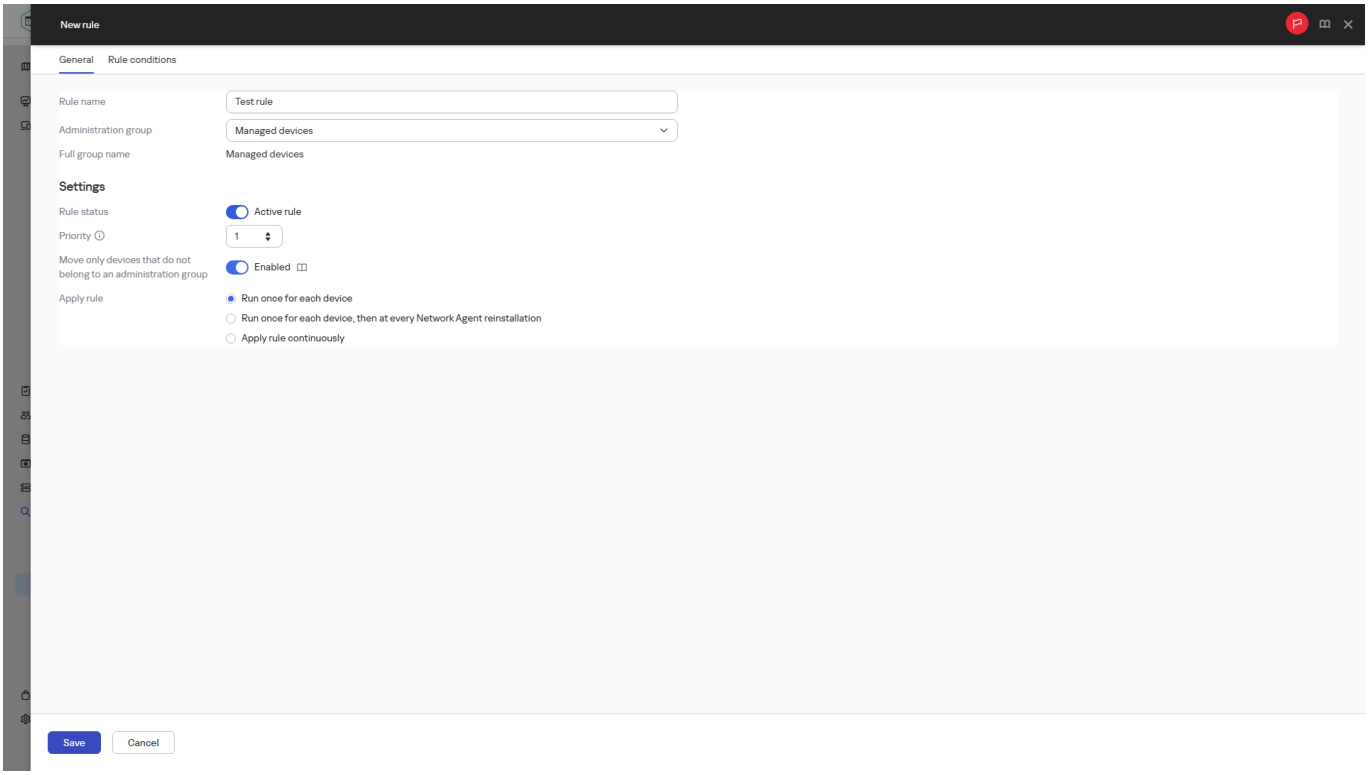
Можно настроить правила перемещения устройств, в соответствии с которыми устройства будут распределены по группам администрирования.

Чтобы создать правило перемещения устройств:

1. В главном окне приложения перейдите в раздел **Управление активами → Правила перемещения**.



2. Нажмите на кнопку **Добавить**. Откроется окно **Новое правило**.



3. В открывшемся окне укажите следующие данные на вкладке **Общие**:

   Имя правила

   Укажите имя нового правила активации.

   Если вы копируете правило, новое правило получает такое же имя, как и исходное правило, но к нему добавляется индекс в скобках, например: (1).

   Группа администрирования

Выберите группу администрирования, в которую будут автоматически перемещаться устройства.

Статус правила

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.

Приоритет

Вы можете указать приоритет правила перемещения. Самый высокий приоритет равен 1. Чем больше значение **Приоритет**, тем ниже приоритет правила и его позиция в списке.

Если приоритет не назначен, правилу назначается самый низкий приоритет.

При копировании правила копии правила присваивается приоритет исходного правила. Приоритет исходного правила увеличивается на 1.

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.

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).

4. На вкладке **Условия правила** укажите хотя бы один критерий, по которому устройства будут перемещены в группу администрирования.

5. Нажмите на кнопку **Сохранить**.

Правило перемещения создано. Оно появится в списке правил перемещения.

Чем выше положение правила в списке, тем выше его приоритет.

Чтобы изменить приоритет:

1. Установите флажок около правила перемещения.
2. Выполните одно из следующих действий:
   - Нажмите на кнопку **Изменить приоритет** и укажите новый приоритет.
   - Переместите правило вверх или вниз по списку с помощью кнопок **Вверх** или **Вниз**.
3. Нажмите на кнопку **Сохранить**.

> 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).

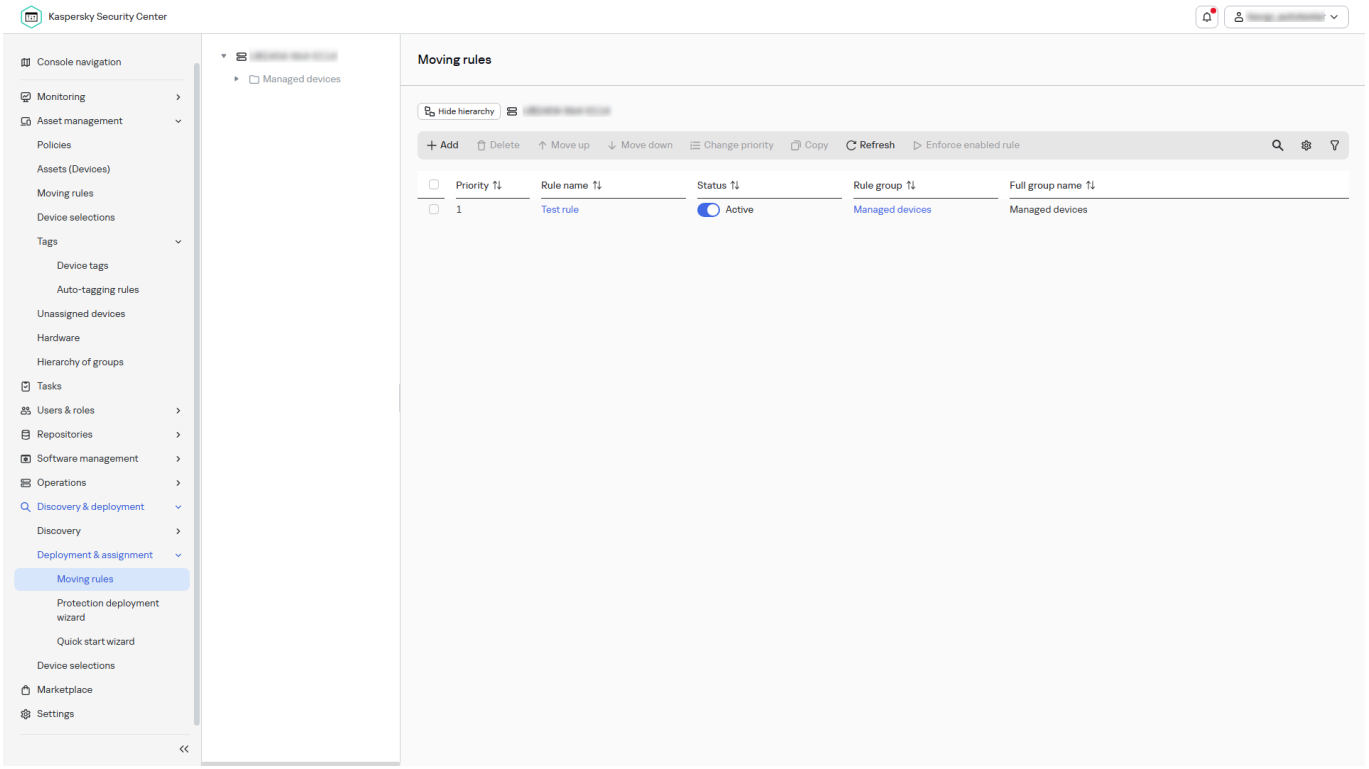
Копирование правил перемещения устройств

Можно копировать правила перемещения устройств, например, если требуется несколько одинаковых правил для разных целевых групп администрирования.

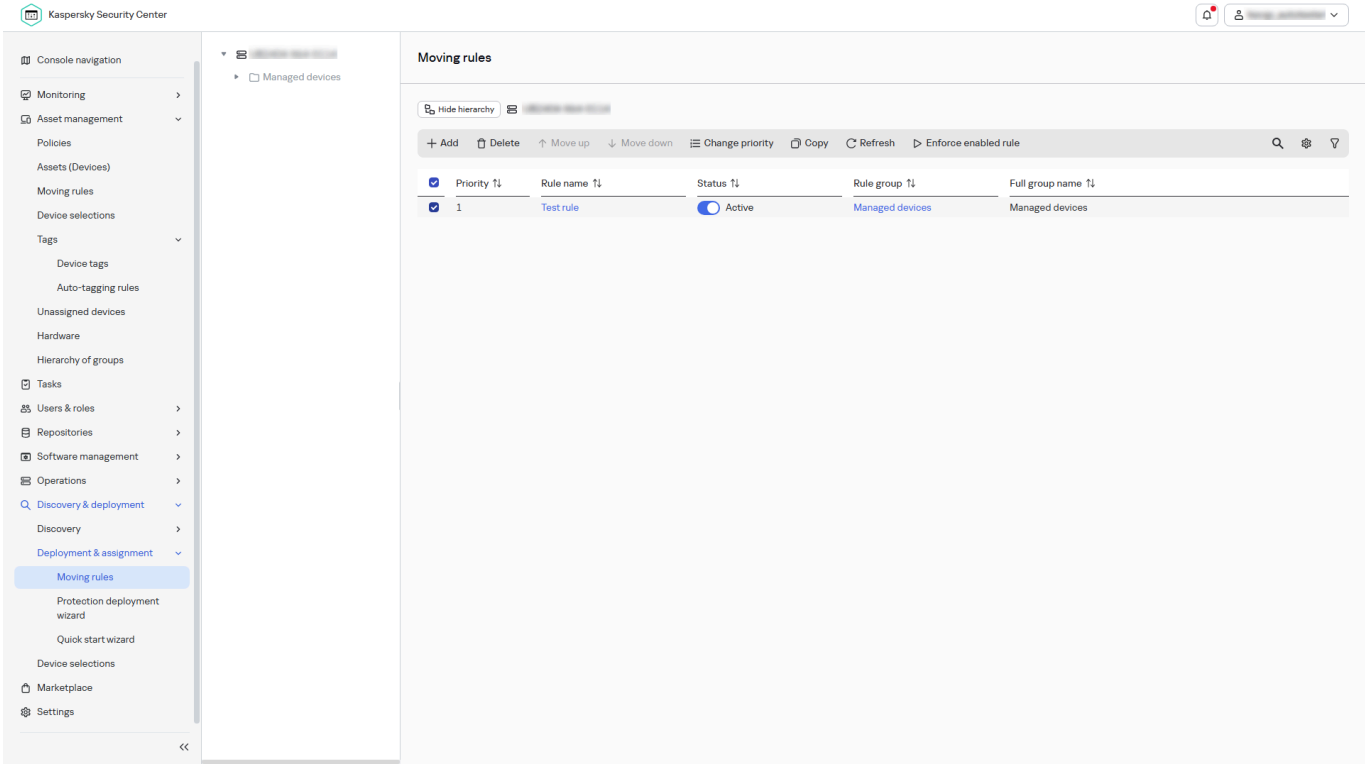
Чтобы скопировать правило перемещения устройств:

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Управление активами → Правила перемещения**.
   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание → Развертывание и назначение → Правила перемещения**.

Отобразится список правил перемещения устройств.



2. Установите флажок напротив правила, которое требуется скопировать.



3. Нажмите на кнопку **Копировать**.

4. В открывшемся окне при необходимости измените данные на вкладке **Общие** либо оставьте существующие значения, если требуется только скопировать правило, без изменения параметров:

   Имя правила

   Укажите имя нового правила активации.

   Если вы копируете правило, новое правило получает такое же имя, как и исходное правило, но к нему добавляется индекс в скобках, например: (1).

   Группа администрирования

Выберите группу администрирования, в которую будут автоматически перемещаться устройства.

Статус правила

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.

Приоритет

Вы можете указать приоритет правила перемещения. Самый высокий приоритет равен 1. Чем больше значение **Приоритет**, тем ниже приоритет правила и его позиция в списке.

Если приоритет не назначен, правилу назначается самый низкий приоритет.

При копировании правила копии правила присваивается приоритет исходного правила. Приоритет исходного правила увеличивается на 1.

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.

Применить правило

Вы можете выбрать один из следующих вариантов:

- **Выполнять один раз для каждого устройства**

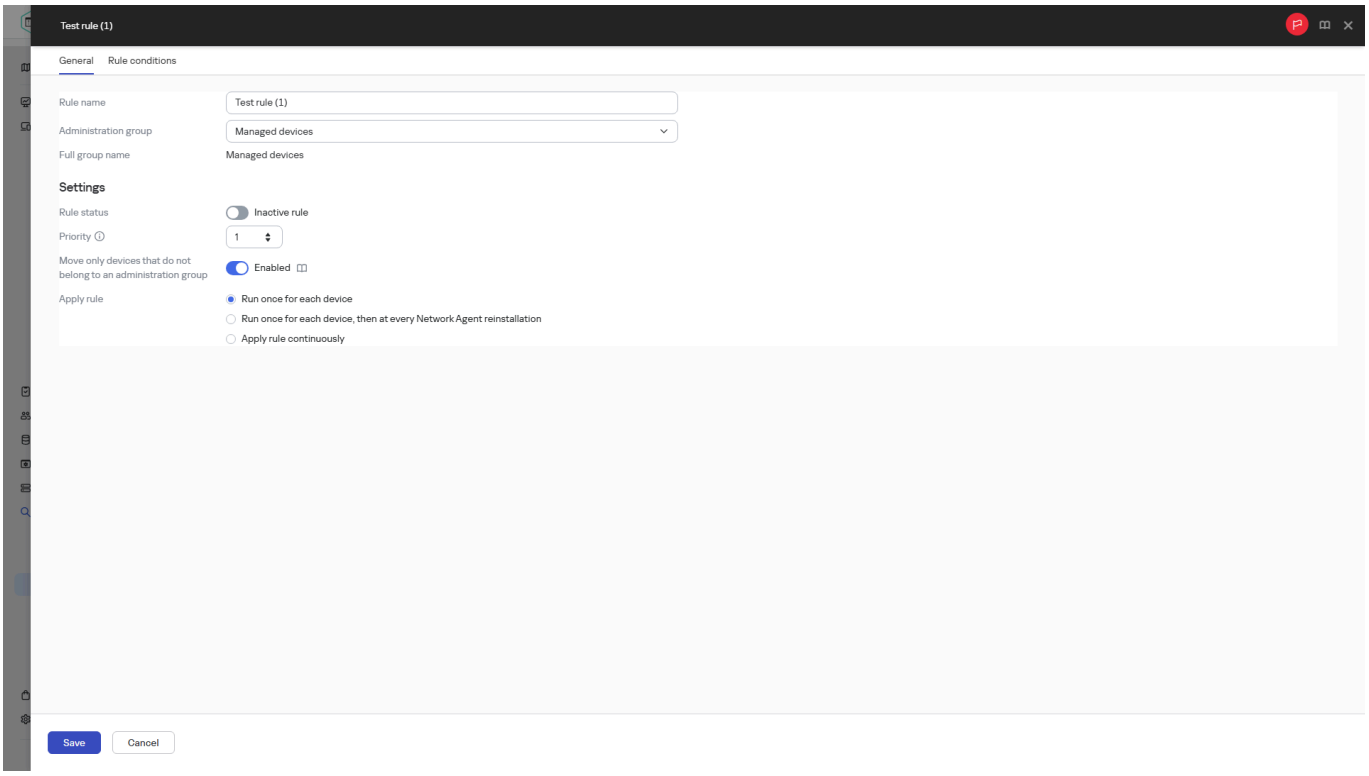
  Правило применяется однократно для каждого устройства, соответствующего указанным критериям.

- **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).



5. На вкладке **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

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.
- Владелец устройства, его роль и членство в группе безопасности.
- Управляемые приложения, установленные на клиентских устройствах, например Агент администрирования или Сервер администрирования.
- Виртуальные машины, которые являются клиентскими устройствами.
- Подразделения контроллеров домена.
- Облачные сегменты.

Ниже вы можете найти описание того, как указать эту информацию в правиле перемещения устройств.

Если в правиле указано несколько условий, срабатывает логический оператор AND и применяются все условия одновременно. Если вы не выберете какие-либо параметры или оставите некоторые поля пустыми, такие условия не применяются.

Вкладка Теги

На этой вкладке можно настроить поиск устройств по ключевым словам (тегам), которые были добавлены ранее в описания клиентских устройств. 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.

Вкладка Сеть

На этой вкладке вы можете указать сетевые данные устройств, которые учитывает правило перемещения устройств:

Имя устройства в сети Windows

Имя устройства в сети Windows (NetBIOS-имя) или IPv4-адрес или IPv6-адрес.

Windows-домен

Правило перемещения устройств применяется ко всем устройствам, включенным в указанный Windows-домен.

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 Linux, 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.

Устройство находится в подгруппе группы "Домены"

Если этот параметр включен, можно выбрать подгруппу группы "Домены". Соответствующие устройства должны быть расположены в выбранной подгруппе.

По умолчанию параметр выключен.

Устройство находится в IP-диапазоне

Если этот параметр включен, вы можете выбрать IP-диапазон, который вы ранее добавили в разделе **IP-диапазоны**. Соответствующие устройства должны быть включены в выбранный IP-диапазон.

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.

Вкладка Владелец устройства

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

Владелец устройства

Выберите имя пользователя владельца устройства из внутренней группы безопасности. Узнайте больше о пользователях и ролях пользователей в этом разделе.

> В качестве владельца устройства может быть зарегистрировано не более одного пользователя.

Членство владельца устройства в группе безопасности Active Directory

Выберите внешнюю группу безопасности Active Directory, к которой принадлежит владелец устройства.

> Пользователь может быть частью группы безопасности Active Directory или частью группы, которая входит в эту группу безопасности Active Directory.

Роль владельца устройства

Выберите роль, назначенную владельцу устройства. Подробнее о ролях пользователей см. в этой статье.

Членство владельца устройства во внутренней группе безопасности

Выберите внутреннюю группу безопасности, к которой принадлежит владелец устройства.

Вкладка Приложения

На этой вкладке можно настроить правило перемещения устройств на основе управляемых приложений 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.

Приложения

Укажите, какие управляемые приложения должны быть установлены на клиентских устройствах, чтобы к этим устройствам применялось правило перемещения устройств. Например, вы можете выбрать **Агент администрирования Kaspersky Security Center 17** или **Сервер администрирования Kaspersky Security Center 17**.

Если вы не выберете управляемое приложение, условие не будет применяться.

Версия ОС

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 ОС

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 какая архитектура используется в операционной системе клиентских устройств:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.
2. Нажмите на кнопку **Параметры столбцов** справа (⚙).
3. Выберите параметр **Архитектура ОС** и нажмите на кнопку **Сохранить**.

   После этого для каждого управляемого устройства отобразится архитектура операционной системы.

ОС менеджера пакетов

Клиентские устройства можно выбирать по менеджеру пакетов операционной системы. В поле **ОС менеджера пакетов** можно выбрать одно из следующих значений:

- rpm – для устройств под управлением операционных систем Red Hat Enterprise Linux, CentOS, Fedora, SUSE, Oracle Linux;
- apt (dpkg) – для устройств под управлением операционных систем Debian, Ubuntu, Kali;
- pkg – для устройств под управлением операционных систем FreeBSD, OpenBSD.

Чтобы проверить какой менеджер пакетов используется в операционной системе клиентских устройств:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.
2. Нажмите на кнопку **Параметры столбцов** справа (⚙).
3. Выберите пункт **ОС менеджера пакетов**, затем нажмите на кнопку **Сохранить**.

   Для каждого управляемого устройства отображается менеджер пакетов, используемый в его операционной системе.

Версия пакета обновления ОС

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 установлено**. Правило перемещения устройств применяется только к мобильным устройствам без мобильного сертификата.
- **Значение не выбрано**. Условие не применяется.

Сборка ОС

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 ОС

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.

Вкладка Виртуальные машины

На этой вкладке можно настроить параметры правила перемещения клиентских устройств в зависимости от того, являются эти устройства виртуальными машинами или частью инфраструктуры виртуальных рабочих столов (VDI):

Является виртуальной машиной

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.

Вкладка Контроллеры домена

На этой вкладке вы можете указать, что требуется перемещать устройства, входящие в организационное подразделение домена. Вы также можете перемещать устройства из всех дочерних подразделений указанного подразделения домена:

Устройство входит в следующее подразделение

Если этот параметр включен, правило перемещения устройств применяется к устройствам из организационного подразделения контроллера домена, указанного в списке под параметром.

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.

Перемещать устройства из дочерних подразделений в соответствующие подгруппы

Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств

Удалять подгруппы, отсутствующие в домене

Устройство включено в следующую группу безопасности домена

Если этот параметр включен, правило перемещения устройств применяется к устройствам из доменной группы безопасности, указанной в списке под параметром.

По умолчанию параметр выключен.

Вкладка Облачные сегменты

На этой вкладке вы можете указать, что требуется перемещать устройства, входящие в облачный сегмент. Вы также можете перемещать устройства из всех дочерних подразделений указанного подразделения домена:

Устройство находится в облачном сегменте

При выборе этого параметра правило перемещения устройств применяется к клиентским устройствам, принадлежащим облачному сегменту. Вы можете выбрать нужный облачный сегмент вплоть до подсети в списке под параметром.

По умолчанию параметр выключен.

Включать дочерние объекты

Если этот параметр включен, в выборку будут включаться устройства, входящие в дочерние подразделения указанного облачного сегмента.

По умолчанию параметр выключен.

Перемещать устройства в соответствующие подгруппы

Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств

Удалять подгруппы, для которых нет соответствия в облачных сегментах

Устройство обнаружено с помощью API

В раскрывающемся списке можно выбрать одно из следующих значений:

- Значение не выбрано. Условие не применяется.
- **Нет**. Перемещаемые устройства, которые не были обнаружены с помощью API.
- **AWS**. Перемещаемые устройства обнаруженные с помощью AWS API.
- **Azure**. Перемещаемые устройства обнаруженные с помощью Azure API.
- **Google Cloud**. Перемещаемые устройства обнаруженные с помощью Google Cloud API.

После этого, в зависимости от выбранного значения, вы можете заполнить следующие поля:

- **Подсеть облачного устройства**.
- **Зона доступности облачного устройства**.
- **Группа размещения облачного устройства**.

Вкладка Пользовательские параметры

> Использование пользовательских параметров доступно только при установленном плагине Kaspersky Mobile Devices Protection and Management 10.59.4.32 или выше.

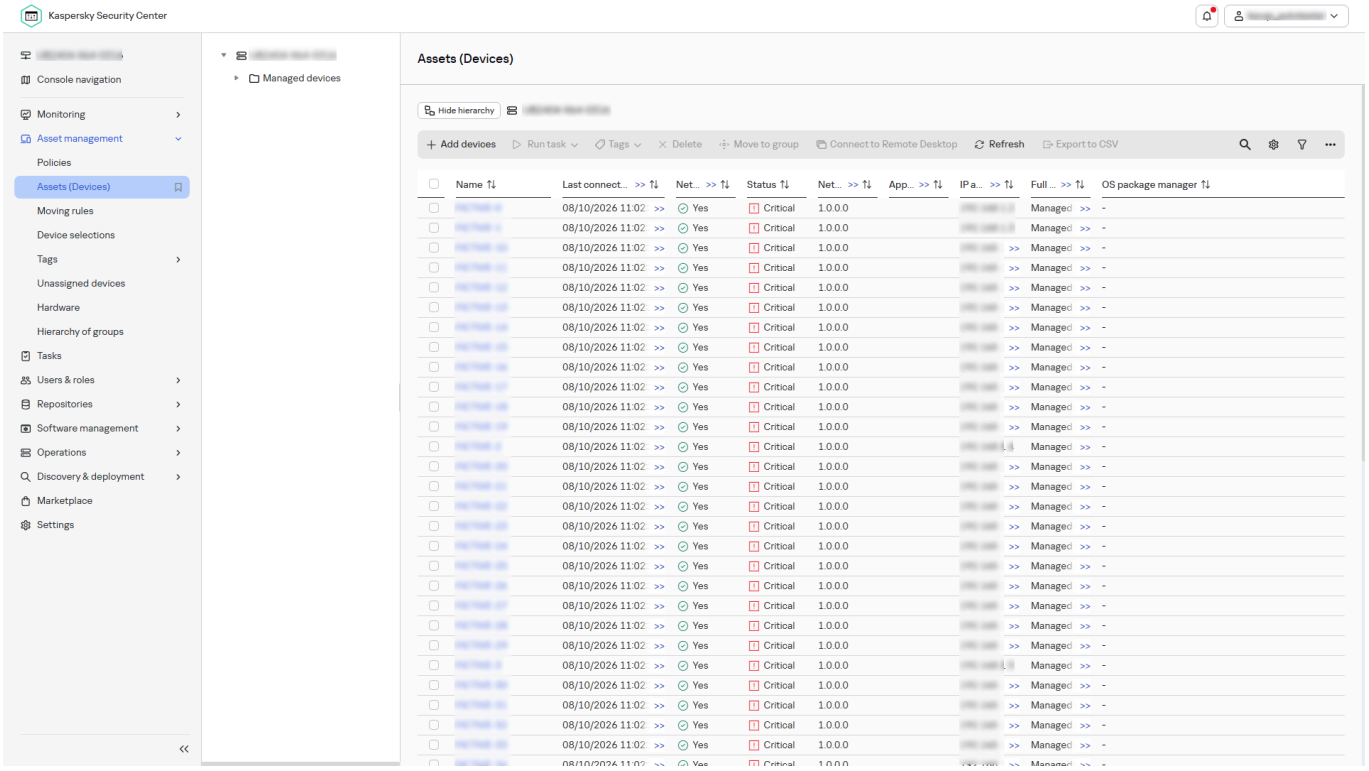
На этой вкладке можно настроить правило перемещения Android-устройств на основе значений пользовательских параметров. Подробная информация об использовании пользовательских параметров представлена в справке Kaspersky Secure Mobility Management.

Добавление устройств в состав группы администрирования вручную

Вы можете перемещать устройства в группы администрирования автоматически, создавая правила перемещения устройств, или вручную, перемещая устройства из одной группы администрирования в другую, или добавляя устройства в выбранную группу администрирования. В этом разделе описано, как вручную добавить устройства в группу администрирования.

Чтобы вручную добавить одно или несколько устройств в состав выбранной группы администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами → Управляемые устройства**.



Список управляемых устройств

2. Выберите группу администрирования, в которую вы хотите добавить устройства:

   - Для корневой группы:

     В этом случае вы можете перейти к следующему шагу.

   - Для подгруппы:

     a. Нажмите на кнопку **Показать иерархию** в верхней части страницы.

        Название кнопки изменится на **Скрыть иерархию**.

     b. В открывшемся окне нажмите на имя подгруппы.

   Путь к выбранной группе отображается в верхней части страницы. При необходимости вы можете нажать на ссылку с именем группы администрирования, чтобы перейти к группе. По умолчанию последняя ссылка в пути неактивна. Также вы можете закрыть окно иерархии, нажав на кнопку **Скрыть иерархию**.

3. Нажмите на кнопку **Добавить устройства**.

   В результате запустится мастер перемещения устройств.

4. 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.

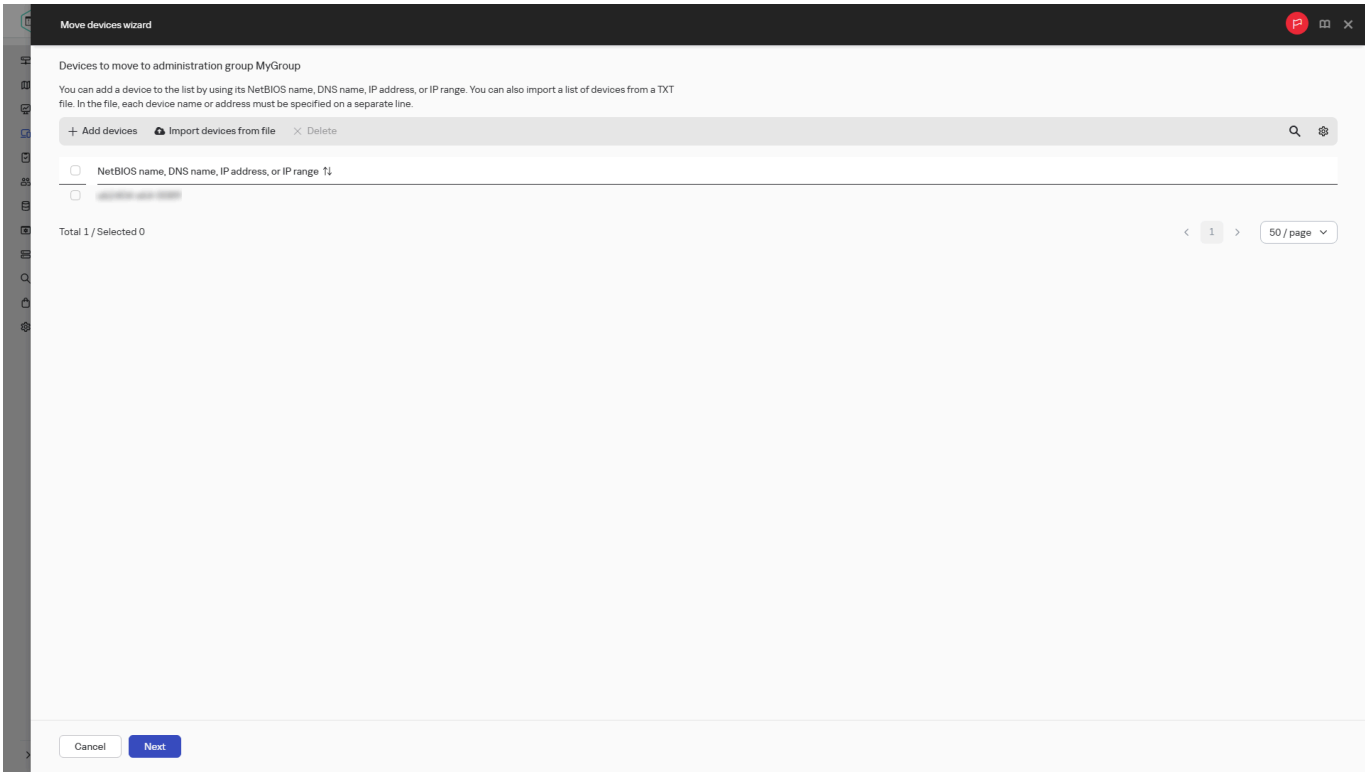
       > IP-диапазон не должен содержать более 1 048 576 адресов.

     - 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: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %



Выбор устройств для перемещения в группу администрирования

5. Просмотрите список устройств, которые будут добавлены в группу администрирования. Вы можете редактировать список, добавляя или удаляя устройства.

6. 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:

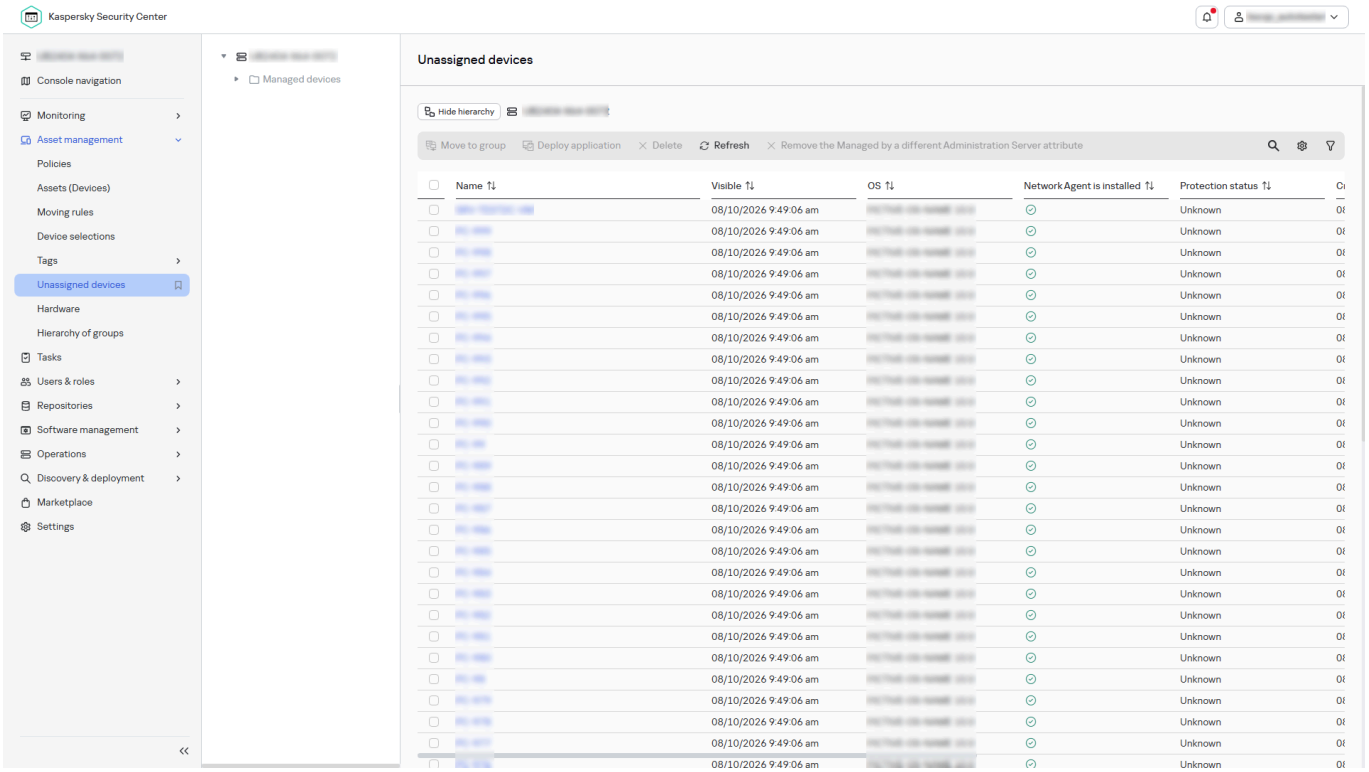
1. Откройте группу администрирования, в которую вы хотите переместить устройства. Для этого выполните одно из следующих действий:

   - Чтобы открыть группу администрирования, в главном меню перейдите в раздел **Управление активами** → **Управляемые устройства** и выберите нужную группу администрирования.

     - Для корневой группы вы можете перейти к следующему шагу.

     - Для подгруппы в верхней части страницы нажмите на кнопку **Показать иерархию** и в открывшемся окне выберите нужную группу администрирования.

   - Чтобы открыть группу **Нераспределенные устройства**, в главном меню перейдите в раздел **Управление активами** → **Нераспределенные устройства**.



Список нераспределенных устройств

2. Если группа администрирования содержит кластеры или массивы серверов, раздел **Управляемые устройства** разделен на две вкладки – **Устройства** и **Кластеры и массивы серверов**. Откройте вкладку объекта, который хотите переместить.

3. Установите флажки рядом с устройствами или кластерами, которые требуется переместить в другую группу.

4. Нажмите на кнопку **Переместить в группу**.

5. В иерархии групп администрирования установите флажок рядом с группой администрирования, в которую вы хотите переместить выбранные устройства или кластеры.

6. Нажмите на кнопку **Переместить**.

Выбранные устройства или кластеры перемещаются в выбранную группу администрирования.

О кластерах и массивах серверов

Kaspersky Security Center Linux поддерживает кластерную технологию. Если Агент администрирования передает Серверу администрирования информацию о том, что приложение, установленное на клиентском устройстве, является частью массива сервера, то клиентское устройство становится узлом кластера.

Если группа администрирования содержит кластеры или массивы серверов, на странице **Управляемые устройства** отображаются две вкладки: одна для отдельных устройств, другая для кластеров и массивов серверов. После обнаружения управляемых устройств в качестве узлов кластера, кластер добавляется как отдельный объект на вкладку **Кластеры и массивы серверов**.

Узлы кластера или массивы серверов перечислены на вкладке **Устройства** вместе с другими управляемыми устройствами. Вы можете просматривать свойства узлов как отдельных устройств и выполнять другие операции, но удалить узел кластера или переместить его в другую группу администрирования отдельно от его кластера невозможно. Вы можете удалить или переместить только весь кластер.

Вы можете выполнять следующие операции с кластерами или массивами серверов:

- Посмотреть свойства.
- Переместить кластер или массив серверов в другую группу администрирования.

  При перемещении кластера или массива серверов в другую группу, все его узлы перемещаются вместе с ним, так как кластер и любой из его узлов всегда принадлежат к одной группе администрирования.
- Удалить.

  Целесообразно удалять кластер или массив серверов только тогда, когда кластер или массив серверов больше не существует в сети организации. Если кластер по-прежнему виден в вашей сети, а Агент администрирования и приложение "Лаборатории Касперского" по-прежнему установлено на узлах кластера, Kaspersky Security Center Linux автоматически возвращает удаленный кластер и его узлы обратно в список управляемых устройств.

Свойства кластеров или массивов серверов

Чтобы просмотреть параметры кластера или массива серверов:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства** → **Кластеры и массивы серверов**.

   Отображается список кластеров и массивов серверов.

2. Нажмите на имя нужного кластера или массива серверов.

Откроется окно свойств выбранного кластера или массива серверов.

Общие

Раздел **Общие** отображает общую информацию о кластере или массиве серверов. Информация предоставляется на основании данных, полученных в ходе последней синхронизации узлов кластера с Сервером администрирования:

Имя

Описание

Windows-домен

Windows-домен или рабочая группа, содержащая кластер или массив серверов.

NetBIOS-имя

Имя кластера или массива серверов в сети Windows.

DNS-имя

Имя DNS-домена кластера или массива серверов.

Задачи

На вкладке **Задачи** вы можете управлять задачами, назначенными для кластеров и массивов серверов: просматривать список существующих задач, создавать новые, удалять, запускать и останавливать задачи, изменять параметры задач и просматривать результаты выполнения. Перечисленные задачи относятся к приложению безопасности "Лаборатории Касперского", установленного на узлах кластера. Kaspersky Security Center Linux получает список задач и информацию о статусе задач от узлов кластера. В случае отсутствия связи статус не отображается.

Узлы

На этой вкладке отображается список узлов, входящих в кластер или массив серверов. Вы можете нажать на имя узла, чтобы просмотреть окно свойств устройства.

Приложения "Лаборатории Касперского"

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

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;
  - опрашивать 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 специально выделенных точек распространения в сети, содержащей один сегмент сети, в зависимости от количества устройств в сети

Число клиентских устройств в сегменте 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 специально выделенных точек распространения в сети, содержащей несколько сегментов сети, в зависимости от количества устройств в сети

Число клиентских устройств в каждом 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 сегменте 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 каждом 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.

Устройства с операционной системой Microsoft Windows на Arm не могут выступать в роли точек распространения.

Чтобы назначить точки распространения автоматически:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.

3. Выберите параметр **Автоматически назначать точки распространения**.

   Если автоматическое назначение устройств точками распространения включено, невозможно вручную настраивать параметры точек распространения, а также изменять список точек распространения.

4. Нажмите на кнопку **Сохранить**.

В результате Сервер администрирования будет автоматически назначать точки распространения и настраивать их параметры.

Назначение точек распространения вручную

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 точек распространения.

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

Устройства с операционной системой Microsoft Windows на Arm не могут выступать в роли точек распространения.

Чтобы вручную назначить устройство точкой распространения:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.

3. Выберите параметр **Вручную назначать точки распространения**.

4. Нажмите на кнопку **Назначить**.

5. Выберите устройство, которое вы хотите сделать точкой распространения.

   При выборе устройства учитывайте особенности работы точек распространения и требования к устройству, которое выполняет роль точки распространения.

6. Выберите группу администрирования, которую вы хотите включить в область действия выбранной точки распространения.

7. Нажмите на кнопку **OK**.

   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 TLS-порта, по которому осуществляется защищенное подключение клиентских устройств к точке распространения с использованием протокола TLS.

     По умолчанию номер порта – 13000.

     Включено

     Если параметр включен, для автоматического распространения инсталляционных пакетов на клиентские устройства в пределах группы будет использоваться многоадресная IP-рассылка.

     Многоадресная IP-рассылка уменьшает время, необходимое для установки приложений из инсталляционного пакета на группу клиентских устройств, но увеличивает время установки при установке приложения на одно клиентское устройство.

     Адрес IP-рассылки

     IP-адрес, на который будет выполняться многоадресная рассылка. IP-адрес можно задать в диапазоне 224.0.0.0 – 239.255.255.255

     По умолчанию Kaspersky Security Center 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 TLS-протокола по умолчанию используется порт 13001.

Адрес точки распространения для удаленных устройств

Сетевой адрес, через который удаленные устройства подключаются к точке распространения.

Включено

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.

Включено

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.

Включено

В Kaspersky Security Center Linux 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.

Скачать файлы различий

Этот параметр включает функцию загрузки файлов различий.

По умолчанию параметр включен.

- Если ваши точки распространения используют прокси-сервер для подключения к интернету, в подразделе **Параметры подключения к интернету** вы можете указать следующие параметры:

  Использовать прокси-сервер

  Если этот флажок установлен, для подключения точек распространения к серверу обновлений "Лаборатории Касперского" используется прокси-сервер в интернете. Вы можете настроить подключение к прокси-серверу в полях ввода.

  По умолчанию флажок снят.

  Адрес прокси-сервера

  Адрес прокси-сервера.

  Номер порта

  Номер порта, по которому будет выполняться подключение.

  Не использовать прокси-сервер для локальных адресов

  Если параметр включен, то при подключении к устройствам в локальной сети не используется прокси-сервер.

  По умолчанию параметр выключен.

  Аутентификация на прокси-сервере

  Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  По умолчанию флажок снят.

  Имя пользователя

  Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.

  Пароль

  Пароль учетной записи, от имени которой будет запускаться задача.

- В разделе **Прокси-сервер KSN** вы можете настроить приложение так, чтобы точка распространения использовалась для пересылки KSN запросов от управляемых устройств.

Включить прокси-сервер KSN на стороне точки распространения

Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского".

По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены в окне свойств Сервера администрирования.

Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

Пересылать KSN запрос Серверу администрирования

Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

По умолчанию параметр включен.

Доступ к облачной службе KSN/KPSN непосредственно через интернет

Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или KPSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или KPSN.

Игнорировать параметры прокси-сервера для подключения к KPSN

Установите этот флажок, если параметры прокси-сервера настроены в свойствах точки распространения или политики Агента администрирования, но ваша архитектура сети требует, чтобы вы использовали KPSN напрямую. В противном случае запрос от управляемого приложения не будет передан в KPSN.

Это параметр доступен, если вы выбрали параметр **Доступ к облачной службе KSN/KPSN непосредственно через интернет**.

Порт

Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.

Использовать UDP-порт

Чтобы управляемые устройства подключались к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и укажите номер UDP-порта. По умолчанию параметр включен.

UDP-порт

Номер UDP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

Использовать HTTPS

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

HTTPS-порт

Номер HTTPS-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию подключение к прокси-серверу KSN выполняется через HTTPS-порт 17111.

- 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 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 TLS-аутентификации, единственный способ распространить сертификат мобильного устройства – это с помощью установочного пакета.

- Настройте опрос сети Windows с помощью точки распространения с операционной системой Windows.

  Windows-домены;

  Вы можете включить обнаружение устройств для Windows-доменов и задать его расписание.

- Настройте опрос контроллеров домена с помощью точки распространения.

  Опрос контроллеров домена

  Вы можете включить обнаружение устройств для контроллеров домена.

  Когда переключатель установлен в положение **Включено**, в поле **Опрос** вы можете выбрать контроллеры домена для опроса, а также указать для них расписание опроса.

  Если вы используете точку распространения с операционной системой Linux, в разделе **Опросить указанные домены** нажмите на кнопку **Добавить**, а затем укажите адрес и учетные данные пользователя контроллера домена. Также вы можете указать тип домена для опроса: Active Directory или Samba, FreeIPA, ALD Pro.

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

  - **Опросить текущий домен**

  - **Опросить весь лес доменов**

  - **Опросить указанные домены**

- Настройте опрос IP-диапазонов точкой распространения.

  Опрос IP-диапазонов.

  Вы можете включить обнаружение устройств для IPv4-диапазонов и IPv6-сетей.

  Если вы включили параметр **Разрешить опрос диапазона**, вы можете добавить диапазон опроса и задать расписание опроса. Вы можете добавить IP-диапазоны в список опрашиваемых диапазонов.

Если включить параметр **Использовать Zeroconf для опроса IPv6-сетей**, точка распространения выполняет опрос IPv6-сети, используя сеть с нулевой конфигурацией (далее также *Zeroconf*). В этом случае указанные IP-диапазоны игнорируются, так как точка распространения опрашивает всю сеть. Параметр **Использовать Zeroconf для опроса IPv6-сетей** доступен, если точка распространения работает под управлением Linux. Чтобы использовать опрос Zeroconf IPv6, вам нужно установить утилиту avahi-browse на точке распространения.

- В разделе **Дополнительно** укажите папку, которую точка распространения должна использовать для хранения распространяемых данных.

  Использовать папку по умолчанию

  При выборе этого варианта для сохранения данных будет использоваться папка, в которую на точке распространения установлен Агент администрирования.

  Использовать указанную папку

  При выборе этого варианта в расположенном ниже поле можно указать путь к папке. Папка может размещаться как локально на точке распространения, так и удаленно, на любом из устройств, входящих в состав сети организации.

  Учетная запись, под которой на точке распространения запускается Агент администрирования, должна иметь доступ к указанной папке для чтения и записи.

10. Нажмите на кнопку **OK**.

В результате выбранные устройства будут выполнять роль точек распространения.

Добавление шлюза соединения в демилитаризованной зоне в качестве точки распространения

Если Сервер администрирования находится вне демилитаризованной зоны (DMZ), Агенты администрирования, установленные на внешних устройствах, теряют возможность соединения с ним. В этом случае вы можете использовать точку распространения в качестве шлюза соединения в демилитаризованной зоне. Точка распространения открывает порт для Сервера администрирования для создания соединения. В момент запуска Сервер администрирования подключается к точке распространения и не разрывает соединение с ней в течение всего времени работы.

Если вам нужно установить соединение между Сервером администрирования и вашими управляемыми устройствами вне периода синхронизации между Агентом администрирования и Сервером администрирования, вам нужно включить push-сервер и открыть порт 13295 на стороне точки распространения.

Рекомендуется использовать в качестве шлюза соединения выделенное устройство. Информацию о максимальном количестве клиентских устройств (включая мобильные) см. в руководстве по масштабированию.

Шлюз соединения ожидает соединений от Сервера администрирования, а не устанавливает соединения с Сервером администрирования. Это означает, что сразу после установки шлюза соединения на устройстве в демилитаризованной зоне Сервер администрирования не перечисляет устройство среди управляемых устройств. Следовательно, вам потребуется особая процедура, чтобы Сервер администрирования инициировал соединение со шлюзом соединения.

Чтобы добавить устройство со шлюзом соединения в качестве точки распространения:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.

3. Выберите параметр **Вручную назначать точки распространения**.

4. В панели инструментов нажмите на кнопку **Назначить**.

5. В открывшейся правой панели выполните следующее:

   a. Выберите вариант **Использовать шлюз соединения в демилитаризованной зоне по адресу**.

   b. В поле **Адрес шлюза соединения** укажите IP-адрес или DNS-имя устройства.

   c. Нажмите на кнопку **Назначить**.

   d. Панель закроется, а точка распространения отобразится с именем **Временная запись для шлюза соединения**.

6. Нажмите на кнопку **Сохранить**.

   Сервер администрирования пытается подключиться к шлюзу соединения по указанному адресу. В случае успеха название записи меняется на имя устройства шлюза соединения. Этот процесс занимает до пяти минут.

Если вы откроете свойства точки распространения, нажав **Временная запись для шлюза соединения**, все параметры будут недоступны. Вы можете просмотреть только вкладку Общие, на которой отображается имя точки распространения. Используется порт по умолчанию (13000). Настроить параметры точки распространения можно только после подключения к ней Сервера администрирования. Пока временная запись для шлюза соединения преобразуется в именованную запись, шлюз соединения также появляется в группе Нераспределенные устройства.

Чтобы добавить шлюз соединения в ранее настроенную сеть:

1. Установите Агент администрирования в режиме шлюза соединения.

2. Переустановите Агент администрирования на устройствах, которые вы хотите подключить к вновь добавленному шлюзу соединения.

Изменение списка точек распространения для группы администрирования

Вы можете просмотреть список точек распространения, назначенных для определенной группы администрирования, и изменить список, добавив или удалив точки распространения.

Чтобы просмотреть и изменить список точек распространения для группы администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.
2. Выберите группу администрирования, для которой вы хотите просмотреть назначенные точки распространения, нажмите на кнопку **Показать иерархию** в верхней части страницы, а затем в открывшемся окне нажмите на имя нужной группы.

   Для этого используйте пункт меню **Точки распространения**.

   Путь к выбранной группе отображается в верхней части страницы. Чтобы перейти к группе администрирования, в этом пути нажмите на ссылку с названием группы. По умолчанию последняя ссылка в пути неактивна.
3. В главном окне приложения перейдите в раздел **Управление активами** → **Точки распространения**.
4. Чтобы добавить точки распространения для группы администрирования, нажмите на кнопку **Назначить**.
5. 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 Linux 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 управляемого приложения или создание туннеля. Если вы используете точку распространения в качестве push-сервера, вам не нужно использовать параметр **Не разрывать соединение с Сервером администрирования** на управляемых устройствах или отправлять пакеты на UDP-порт Агента администрирования.

Push-сервер поддерживает нагрузку до 50 000 одновременных подключений.

Чтобы включить push-сервер на точке распространения:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На вкладке **Общие** выберите раздел **Точки распространения**.
3. Нажмите на имя точки распространения, на которой вы хотите включить push-сервер.

   Откроется окно свойств точки распространения.

4. В разделе **Общие** включите параметр **Включено**.

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 **OK**.

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 с операционной системой Linux, выполняющем роль точки распространения, выполните следующую команду:

   ```
   systemctl edit klnagent64.service
   ```

2. Укажите жесткие и мягкие ограничения файловых дескрипторов в параметре `LimitNOFILE` в секции `[Service]`:

   ```
   LimitNOFILE=<soft resource limits>:<hard resource limits>
   ```

   Например, `LimitNOFILE=32768:131072`. Обратите внимание, что мягкие ограничения дескрипторов файлов должны быть меньше или равны жесткому ограничению.

3. 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: Failed to parse resource value, ignoring: 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: Soft resource limit chosen higher than hard limit, ignoring: 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.

4. Выполните следующую команду, чтобы перезагрузить процесс systemd:

   ```
   systemctl daemon-reload
   ```

5. Выполните следующую команду, чтобы перезапустить службу Агента администрирования:

   ```
   systemctl restart klnagent
   ```

6. Выполните следующую команду, чтобы убедиться, что указанные параметры применяются правильно:

   ```
   less /proc/<nagent process id>/limits
   ```

   где параметр `<nagent process 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.

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). 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*. 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*.
- *OK* или *OK/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
Приложение безопасности не установлено	Агент администрирования установлен на устройстве, но не установлено приложение безопасности.	• Переключатель включен. • Переключатель выключен.
Обнаружено много вирусов	В результате работы задач поиска вирусов, например, задачи Поиск вредоносного ПО, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение.	Более 0.
Уровень постоянной защиты отличается от уровня, установленного администратором	Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства.	• Остановлена. • Приостановлена. • Выполняется.
Давно не выполнялся поиск вредоносного ПО	Устройство видимо в сети и на устройстве установлено приложение безопасности, но ни задача *Поиск вредоносного ПО*, ни задача локальной проверки не выполнялись больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее.	Более 1 дня.
Базы устарели	Устройство видимо в сети и на устройстве установлено приложение безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее.	Более 1 дня.
Давно не подключались	Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено.	Более 1 дня.

Условие	Описание условия	Доступные значения
Обнаружены активные угрозы	Количество необработанных объектов в папке **Активные угрозы** превышает указанное значение.	Более чем 0 штук.
Время, прошедшее с момента перезапуска	Устройство видимо в сети, но перезапуск требуется приложением уже дольше указанного интервала времени.	Более чем 0 минут.
Причина перезапуска	Устройство видимо в сети, но приложению требуется перезагрузка устройства по одной из выбранных причин.	• Неизвестная причина • Приложение неработоспособно до перезагрузки • Для завершения обновления требуется перезагрузка; приложение работоспособно • Для инициации обновления требуется перезагрузка • Для завершения проверки или лечения требуется перезагрузка • Требуется перезагрузка для завершения удаленной установки или удаления • Завершение шифрования данных на диске
Установлены несовместимые приложения	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые приложения.	• Переключатель выключен. • Переключатель включен.
Обнаружены уязвимости в приложениях	Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи *Поиск уязвимостей и требуемых обновлений* на устройстве обнаружены уязвимости в приложениях с заданным уровнем критичности.	• Предельный. • Высокий. • Средний. • Игнорировать, если невозможно закрыть уязвимость. • Игнорировать, если обновление назначено к установке.
Срок действия лицензии истек	Устройство видимо в сети, но срок действия лицензии истек.	• Переключатель выключен. • Переключатель включен.
Срок действия лицензии скоро истекает	Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.	Более чем 0 дней.

Условие	Описание условия	Доступные значения
Давно не выполнялась проверка обновлений Центра обновления Windows	Устройство видимо в сети, но задача *Поиск уязвимостей и требуемых обновлений* не выполнялась больше указанного времени.	Более 1 дня.
Недопустимый статус шифрования	Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению.	• Не соответствует политике из-за отказа пользователя (только для внешних устройств). • Не соответствует политике из-за ошибки. • В процессе применения политики – требуется перезагрузка. • Не задана политика шифрования. • Не поддерживается. • В процессе применения политики.
Параметры мобильного устройства не соответствуют политике	Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия.	• Переключатель выключен. • Переключатель включен.
Есть необработанные проблемы безопасности	На устройстве есть необработанные проблемы безопасности. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором.	• Переключатель выключен. • Переключатель включен.
Статус устройства определен приложением	Статус устройства определяется управляемым приложением. Управляемые устройства могут иметь статус, определяемый управляемыми приложениями, независимо от параметров Kaspersky Security Center Linux. После того как этот статус вернет один из статусов, определенных Kaspersky Security Center Linux, Сервер администрирования Kaspersky Security Center присваивает управляемому устройству предельный статус из тех, которые были возвращены управляемым приложением и присвоены Сервером администрирования Kaspersky Security Center. Статусы устройств определенные приложениями имеют описания, переданные управляемыми приложениями. Вы можете просмотреть описания в списке управляемых устройств в столбце **Описание статуса**.	• 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 приложение безопасности на устройстве отключено больше указанного времени. В этом случае состояние приложения безопасности *Остановлено* или *Сбой* и отличается от следующих: *Запускается*, *Выполняется* или *Приостановлена*.	Более чем 0 минут.
Приложение безопасности не запущено	Устройство видимо в сети и приложение безопасности установлено на устройстве, но не запущено.	• 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.

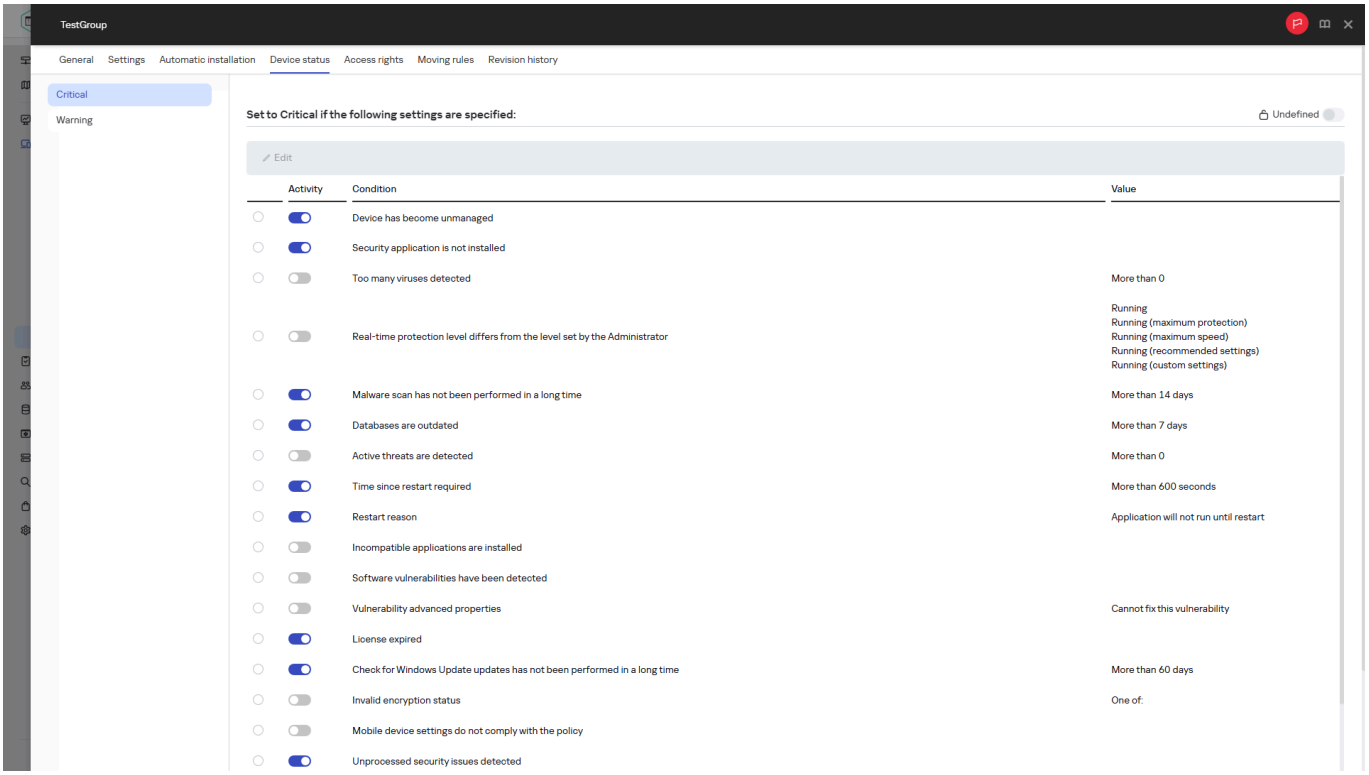
Настройка переключения статусов устройств

Вы можете изменить условия присвоения статусов *Критический* или *Предупреждение* устройству.

Чтобы изменить статус устройства на Критический:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп**.
2. Перейдите в свойства группы администрирования, для которой вы хотите изменить статусы устройств, одним из следующих способов:
   - Выберите имя группы администрирования.
   - Нажмите на кнопку **Показать иерархию** в верхней части страницы. В открывшейся панели наведите курсор мыши на название нужной группы и нажмите на значок параметров (⚙).

   Откроется окно свойств группы администрирования.
3. В окне свойств выберите вкладку **Статус устройства**.
4. Выберите раздел **Критический**.
5. В блоке **Установить статус "Критический", если** включите условие, чтобы перевести устройство в состояние *Критическое*.



Вы можете изменить только 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**.
10. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

При выполнении заданных условий управляемому устройству присваивается статус *Критический*.

Чтобы изменить статус устройства на Предупреждение:

1. В главном окне приложения перейдите в раздел **Управление активами → 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 вкладку **Статус устройства**.
4. Выберите раздел **Предупреждение**.
5. В блоке **Установить статус "Предупреждение", если**, включите условие, чтобы переключить устройство в состояние *Предупреждение*.

   Вы можете изменить только 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**.
10. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

При выполнении заданных условий управляемому устройству присваивается статус *Предупреждение*.

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 Linux предоставляет широкий диапазон *предопределенных выборок устройств* (например, **Устройства со статусом "Критический"**, **Защита выключена**, **Обнаружены активные угрозы**). Предопределенные выборки невозможно удалить. Вы можете также создавать и настраивать дополнительные *пользовательские выборки событий*.

В пользовательских выборках вы можете задать область поиска и выбрать все устройства, управляемые устройства или нераспределенные устройства. Параметры поиска задаются в условиях. В выборках устройств вы можете создать несколько условий с различными параметрами поиска. Например, вы можете создать два условия и задать различные IP-диапазоны в каждом из них. Если задано несколько условий, в выборку устройств попадут устройства, которые удовлетворяют любому из условий. Напротив, параметры поиска в одном условии накладываются друг на друга. Если в условии выборки заданы IP-диапазон и название установленного приложения, то в выборку устройств попадут только те устройства, на которых одновременно установлено указанное приложение и их IP-адреса входят в указанный диапазон.

Просмотр списка устройств из выборки устройств

Kaspersky Security Center Linux позволяет просматривать список устройств из выборки устройств.

Чтобы просмотреть список устройств из выборки устройств:

1. В главном окне приложения перейдите в раздел **Управление активами** → **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.

Также вы можете запускать задачи для устройств выборки. Для этого выберите одно или несколько устройств, затем нажмите на кнопку **Запустить задачу** и выберите: **Создать задачу**, которая будет применена к этим устройствам, либо **Использовать существующую задачу**.

Чтобы переместить выбранные устройства из выборки устройств в другую группу администрирования, нажмите на кнопку **Переместить в группу** и выберите целевую группу администрирования.

Создание выборки устройств

Чтобы создать выборку устройств:

1. В главном окне приложения перейдите в раздел **Управление активами** → **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 **Сохранить**.

7. Нажмите на кнопку **Сохранить**.

Выборка устройств создана и добавлена в список выборок устройств.

Настройка выборки устройств

Чтобы настроить параметры выборки устройств:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Выборки устройств**.

   Отобразится страница со списком выборок устройств.

2. Выберите соответствующую пользовательскую выборку устройств и нажмите на кнопку **Свойства**.

   Откроется окно **Параметры выборки устройств**.

3. На вкладке **Общие** перейдите по ссылке **Новое условие**.

4. Укажите условия, которые должны быть выполнены, чтобы устройство было включено в эту выборку.

5. Нажмите на кнопку **Сохранить**.

   Параметры применены и сохранены.

Ниже описаны параметры условий отнесения устройств к выборке. Условия сочетаются по логическому "или": в выборку попадают устройства, удовлетворяющие хотя бы одному из представленных условий.

Общие

В разделе **Общие** можно изменить имя условия выборки и указать, необходимо ли инвертировать это условие:

Инвертировать условие выборки

По умолчанию параметр выключен.

Если вы включите этот параметр, заданное условие выборки будет инвертировано. В выборку попадут все устройства, не соответствующие условию.

В следующем примере показана логика работы инверсии:

- **Условие**: на вашем устройстве установлена операционная система с типом Linux и номером сборки 00.0.000.
- **Инвертированное состояние**: на вашем устройстве установлена операционная система с НЕ (тип Linux и номер сборки 00.0.000), что эквивалентно следующему:

  Есть операционная система с типом НЕ Linux ИЛИ с номером сборки НЕ 00.0.000.

Таким образом, выборка будет включать устройства с операционной системой, например, с типом Windows и номером сборки 00.0.000 или типом Linux и любым номером сборки, отличным от 00.0.000.

Инфраструктура сети

В разделе **Сеть** можно настроить критерии включения устройств в выборку на основании их сетевых данных:

Имя устройства

Имя устройства в сети Windows (NetBIOS-имя) или IPv4-адрес или IPv6-адрес.

Домен

Отображаются все устройства, входящие в указанную рабочую группу.

Группа администрирования

Будут отображаться устройства, входящие в указанную группу администрирования.

Описание

Текст, который содержится в окне свойств устройства: в поле **Описание** раздела **Общие**.

Для описания текста в поле **Описание** допустимо использовать следующие символы:

- Внутри одного слова:
  - *****. Заменяет любую строку длиной 0 и более символов.

  Пример:

  Для описания слов **Сервер**, **Серверный** или Серверная можно использовать строку **Сервер***.

  - **?.** Заменяет любой один символ.

  Пример:

  Для описания таких фраз, как **SUSE Linux корпоративный сервер 12** или же **SUSE Linux корпоративный сервер 15**, можно ввести **SUSE Linux Enterprise Server 1?**.

  Звездочка (*****) или вопросительный знак (**?**) не могут использоваться как первый символ в описании текста.

- Для связи нескольких слов:
  - Пробел. Отображает все устройства, описания которых содержат любое из перечисленных слов.

  Пример:

  Для описания фразы, содержащей слово **Подчиненный** или **Виртуальный** можно использовать строку **Подчиненный Виртуальный**.

  - **+**. При написании перед словом обозначает обязательное наличие слова в тексте.

  Пример:

  Для описания фразы, содержащей и слово **Подчиненный**, и слово **Виртуальный**, можно использовать строку **+Подчиненный+Виртуальный**.

  - **-**. При написании перед словом обозначает обязательное отсутствие слова в тексте.

  Пример:

  Для описания фразы, в которой должно присутствовать слово **Подчиненный**, но должно отсутствовать слово **Виртуальный**, можно использовать строку **+Подчиненный-Виртуальный**.

  - **"<фрагмент текста>"**. Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте.

  Пример:

  Для описания фразы, содержащей словосочетание **Подчиненный Сервер**, можно использовать строку **"Подчиненный Сервер"**.

IP-диапазон

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

По умолчанию параметр выключен.

Под управлением другого Сервера администрирования

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 **Контроллеры домена** можно настроить критерии включения устройств в выборку по членству в домене:

Устройство в подразделении домена

Если этот параметр включен, в выборку будут включаться устройства из подразделения домена, указанного в поле ввода.

По умолчанию параметр выключен.

Это устройство является членом группы безопасности домена

Если этот параметр включен, в выборку будут включаться устройства из группы безопасности домена, указанной в поле ввода.

По умолчанию параметр выключен.

В разделе **Действия в сети** 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**. Приложение включает в выборку устройства, которые видимы в сети в настоящий момент.
- **Нет**. Приложение включает в выборку устройства, которые не видимы в сети в настоящий момент.
- **Значение не выбрано**. Критерий не применяется.

Статусы устройств

В разделе **Статус управляемых устройств** можно настроить критерии включения устройств в выборку по описанию статуса устройства от управляемого приложения:

Статус устройства

Раскрывающийся список, в котором можно выбрать один из статусов устройства: *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.

Device status description

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

Статус защиты данных от утечек

Поиск устройств по статусу компонента защиты от утечки данных (*Нет данных, Остановлена, Запускается, Приостановлена, Выполняется, Сбой*).

Статус защиты для серверов совместной работы

Поиск устройств по статусу защиты для серверов совместной работы (*Нет данных*, *Остановлена*, *Запускается, Приостановлена*, *Выполняется*, *Сбой*).

Статус антивирусной защиты почтовых серверов

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

Статус Endpoint Sensor

Поиск устройств по статусу компонента Endpoint Sensor (*Нет данных, Остановлена, Запускается, Приостановлена, Выполняется, Сбой*).

В разделе **Проблемы, связанные со статусом управляемых приложений** можно настроить критерии включения устройств в выборку в соответствии со списком возможных проблем, обнаруженных управляемым приложением. Если на устройстве существует хотя бы одна проблема, которую вы выбирали, устройство будет включено в выборку. Когда вы выбираете проблему, указанную для нескольких приложений, у вас есть возможность автоматически выбрать эту проблему во всех списках.

Вы можете установить флажки для описаний статусов от управляемого приложения, при получении которых устройства будут включаться в выборку. Когда вы выбираете статус, указанный для нескольких приложений, у вас есть возможность автоматически выбирать этот статус во всех списках.

Сведения о системе

В разделе **ОС** 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 ОС

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 ОС

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.

Сборка ОС

> 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 ОС

> 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 приложениях сторонних производителей

В разделе **Реестр приложений** можно настроить критерии включения устройств в выборку в зависимости от того, какие приложения на них установлены:

Название приложения

Раскрывающийся список, в котором можно выбрать приложение. Устройства, на которых установлено указанное приложение, будут включены в выборку.

Версия приложения

Поле ввода, в котором указывается версия выбранного приложения.

Поставщик

Раскрывающийся список, в котором можно выбрать производителя установленного на устройстве приложения.

Статус приложения

Раскрывающийся список, в котором можно выбрать статус приложения (*Установлено*, *Не установлено*). Устройства, на которых указанное приложение установлено или не установлено, в зависимости от выбранного статуса, будут включены в выборку.

Искать по обновлению

Если этот параметр включен, поиск будет выполняться по данным об обновлении приложений, установленных на искомых устройствах. После установки этого флажка вместо полей **Название приложения**, **Версия приложения** и **Статус приложения** будут отображаться поля **Имя обновления**, **Версия обновления** и **Статус** соответственно.

По умолчанию параметр выключен.

Название несовместимого приложения безопасности

Раскрывающийся список, в котором можно выбрать приложения безопасности сторонних производителей. Во время поиска устройства, на которых установлено выбранное приложение, будут включены в выборку.

Тег приложения

В раскрывающемся списке можно выбрать тег приложения. Все устройства, на которых установлены приложения, имеющие выбранный тег в описании, включаются в выборку устройств.

Применить к устройствам без выбранных тегов

Если параметр включен, в выборку будут включены устройства, в описании которых нет выбранных тегов.

Если этот параметр выключен, критерий не применяется.

По умолчанию параметр выключен.

В разделе **Уязвимости и обновления** можно настроить критерии включения устройств в выборку по источнику обновлений Центра обновления Windows:

WUA переключен на Сервер администрирования

В раскрывающемся списке можно выбрать один из следующих вариантов поиска:

- **Да**. Если выбран этот вариант, в результаты поиска включаются устройства, которые получают обновления Центра обновления Windows с Сервера администрирования.
- **Нет**. Если выбран этот вариант, в результаты включаются устройства, которые получают обновления Центра обновления Windows из другого источника.

Информация о приложениях "Лаборатории Касперского"

В разделе **Приложения "Лаборатории Касперского"** можно настроить критерии включения устройств в выборку на основании выбранного управляемого приложения:

Название приложения

В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске по наименованию приложения "Лаборатории Касперского".

В списке представлены названия только тех приложений, для которых на рабочем месте администратора установлены плагины управления.

Если приложение не выбрано, то критерий не применяется.

Версия приложения

В поле ввода можно указать критерий включения устройств в состав выборки при поиске по номеру версии приложения "Лаборатории Касперского".

Если номер версии не указан, то критерий не применяется.

Название критического обновления

В поле ввода можно указать критерий включения устройств в состав выборки при поиске по установленному для приложения наименованию или номеру пакета обновления.

Если поле не заполнено, то критерий не применяется.

Статус приложения

Раскрывающийся список, в котором можно выбрать статус приложения (*Установлено*, *Не установлено*). Устройства, на которых указанное приложение установлено или не установлено, в зависимости от выбранного статуса, будут включены в выборку.

Выбор периода последнего обновления модулей

С помощью этого параметра можно задать критерий поиска устройств по времени последнего обновления модулей приложений, установленных на устройствах.

Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее обновление модулей приложений, установленных на устройствах.

Если флажок снят, то критерий не применяется.

По умолчанию флажок снят.

Устройство находится под управлением Сервера администрирования

В раскрывающемся списке можно включить в состав выборки устройства, которые находятся под управлением Kaspersky Security Center Linux:

- **Да**. Приложение включает в выборку устройства, которые находятся под управлением Kaspersky Security Center Linux.
- **Нет**. Приложение включает в выборку устройства, которые не находятся под управлением Kaspersky Security Center Linux.
- **Значение не выбрано**. Критерий не применяется.

Приложение безопасности установлено

В раскрывающемся списке можно включить в состав выборки устройства, на которых установлено приложение безопасности:

- **Да**. Приложение включает в выборку устройства, на которых установлено приложение безопасности.
- **Нет**. Приложение включает в выборку устройства, на которых не установлено приложение безопасности.
- **Значение не выбрано**. Критерий не применяется.

В разделе **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 вредоносного ПО. В полях ввода можно указать интервал, в течение которого поиск вредоносного ПО выполнялся в последний раз.

По умолчанию параметр выключен.

Обнаружены угрозы

Если этот параметр включен, поиск клиентских устройств выполняется по количеству найденных вирусов. В полях ввода можно задать нижнее и верхнее значения количества найденных вирусов.

По умолчанию параметр выключен.

В подразделе **Шифрование** можно настроить критерии включения устройств в выборку на основе выбранного алгоритма шифрования:

Алгоритм шифрования

Стандарт симметричного алгоритма блочного шифрования Advanced Encryption Standard (AES). В раскрывающемся списке вы можете выбрать размер ключа шифрования (56 Бит, 128 Бит, 192 Бит или 256 Бит).

Доступные значения: *AES56*, *AES128*, *AES192*, и *AES256*.

Подраздел **Компоненты приложения** содержит список компонентов тех приложений, которые имеют соответствующие плагины управления, установленные в Kaspersky Security Center Web Console.

В разделе **Компоненты приложения** вы можете задать критерий для включения устройств в выборку в соответствии с номерами версий компонентов, относящихся к выбранному приложению:

Статус

Поиск устройств в соответствии со статусом компонента, отправленным управляемым приложением 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 приложения, установленный на управляемом устройстве, имеет указанный статус, устройство входит в выборку устройств.

Статусы, отправленные приложениями:

- *Остановлено* – компонент отключен и в данный момент не работает.
- *Приостановлено* – компонент приостановлен, например, после того, как пользователь приостановил защиту в управляемом приложении.
- *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 приложения.
- *Не поддерживается лицензией* – лицензия не распространяется на выбранный компонент.

В отличие от других статусов, статус *Нет данных от устройства* не отправляется управляемым приложением. Этот параметр показывает, что приложения не имеют информации о выбранном статусе компонента. Например, это может произойти, если выбранный компонент не принадлежит ни одному из приложений, 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.

Все устройства, имеющие этот тег

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.

Все устройства, не имеющие этого тега

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.

Владелец устройства

В разделе **Владелец устройства** вы можете настроить критерии включения устройств в выборку в соответствии с зарегистрированными владельцами устройства, их ролями и их членством в группах безопасности:

Владелец устройства

Выберите имя пользователя владельца устройства из внутренней группы безопасности. Узнайте больше о пользователях и ролях пользователей в этом разделе.

> В качестве владельца устройства может быть зарегистрировано не более одного пользователя.

Членство владельца устройства в группе безопасности Active Directory

Выберите внешнюю группу безопасности Active Directory, к которой принадлежит владелец устройства.

> Пользователь может быть частью группы безопасности Active Directory или частью группы, которая входит в эту группу безопасности Active Directory.

Роль владельца устройства

Выберите роль, назначенную владельцу устройства. Подробнее о ролях пользователей см. в этой статье.

Членство владельца устройства во внутренней группе безопасности

Выберите внутреннюю группу безопасности, к которой принадлежит владелец устройства.

Пользовательские параметры

Использование пользовательских параметров доступно только при установленном плагине Kaspersky Mobile Devices Protection and Management 10.59.4.32 или выше.

В разделе **Пользовательские параметры** можно настроить критерии включения Android-устройств в выборку на основе значений пользовательских параметров. Подробная информация об использовании пользовательских параметров представлена в справке Kaspersky Secure Mobility Management.

Экспорт списка устройств из выборки устройств

Kaspersky Security Center Linux позволяет сохранять информацию об этих устройствах из выборки устройств и экспортировать ее в файл CSV или TXT.

Чтобы экспортировать список устройств из выборки устройств:

1. Откройте таблицу с устройствами из выборки устройств.
2. Используйте один из следующих способов для выбора устройств, которые вы хотите экспортировать:
   - Чтобы выбрать определенные устройства, установите флажки рядом с ними.
   - Чтобы выбрать все устройства на текущей странице таблицы, установите флажок в заголовке таблицы устройств, а затем установите флажок **Выбрать все на текущей странице**.
   - Чтобы выбрать все устройства из таблицы, установите флажок в заголовке таблицы устройств, а затем выберите **Выбрать все**.
3. Нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**. Вся информация о выбранных устройствах, включенных в таблицу, будет экспортирована.

Обратите внимание, если вы отфильтровали таблицу устройств, будут экспортированы только отфильтрованные данные отображаемых столбцов.

Удаление устройств из групп администрирования в выборке

При работе с выборкой устройств вы можете удалять устройства из групп администрирования прямо в выборке, не переходя к работе с группами администрирования, из которых требуется удалить устройства.

Чтобы удалить устройства из групп администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами → Выборки устройств** или **Обнаружение устройств и развертывание → Выборки устройств**.

2. В списке выборок нажмите на имя выборки устройств.

   На странице отображается таблица с информацией об устройствах, включенных в выборку устройств.

3. Выберите устройства, которые вы хотите удалить и нажмите на кнопку **Удалить**.

   В результате выбранные устройства будут удалены из групп администрирования, в которые они входили.

Теги устройств

Kaspersky Security Center Linux позволяет назначать *теги* устройствам. Тег представляет собой строковое значение, которое можно использовать для группировки, описания или 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. Если вы хотите отметить отдельное устройство, вы можете назначить тег вручную. Автоматическое назначение тегов выполняется Kaspersky Security Center Linux одним из следующих способов:

- В соответствии с указанными правилами назначения тегов.
- В соответствии с указанным приложением.

> Не рекомендуется использовать разные способы назначения тегов для назначения одного и того же тега. Например, если тег назначается правилом, не рекомендуется назначать этот тег устройствам вручную.

Если теги назначаются правилами, устройствам назначаются теги автоматически при соблюдении указанных правил. Каждому тегу соответствует отдельное правило. Правила могут применяться к сетевым свойствам устройства, операционной системе, установленным на устройстве приложениям и другим свойствам устройства. Например, вы можете настроить правило, в соответствии с которым устройствам, работающим под управлением операционной системы CentOS, назначается тег `[CentOS]`. Затем можно использовать этот тег при создании выборки устройств, чтобы отобрать все устройства под управлением операционной системы CentOS и назначить им задачу.

> Вы можете добавить только одно правило автоматического назначения тегов для каждого тега. Если вы создадите еще одно правило для того же тега, предыдущее правило будет заменено.

Тег автоматически удаляется с устройства в следующих случаях:

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

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

Создание тегов устройств

Чтобы создать тег устройства:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Теги устройств**.
2. На вкладке **Теги устройств** 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 приложения перейдите в раздел **Хранилища** → **Теги устройств**.
2. На вкладке **Теги устройств** 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

Вы можете удалить только теги, назначенные вручную.

Чтобы удалить тег устройства, назначенный вручную:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Теги устройств**.

   Отобразится список тегов.
2. На вкладке **Теги устройств** 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.

При удалении тега, назначенного устройству автоматически, правило не удаляется, и тег будет назначен новому устройству, когда устройство впервые соответствует условиям правила. Если вы удалите правило автоматического назначения тега, указанный в условиях правила, будет удален со всех устройств, которым он был назначен, но не будет удален из списка тегов. При необходимости вы можете вручную удалить тег из списка.

Удаленный тег не удаляется автоматически с устройства, если этот тег назначен устройству приложением или Агентом администрирования. Для того чтобы управлять такими тегами, используйте утилиту klscflag.

Просмотр устройств, которым назначен тег

Чтобы просмотреть устройства с назначенными тегами:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Теги устройств**.

2. На вкладке **Теги устройств** перейдите по ссылке **Просмотреть устройства** рядом с названием тега, для которого вы хотите посмотреть список назначенных устройств.

   Вы будете перенаправлены в раздел **Управляемые устройства** главного меню с устройствами, отфильтрованными по тегу, для которого вы нажали ссылку **Просмотреть устройства**.

3. Если вы хотите вернуться к списку тегов устройства, нажмите на кнопку **Назад** в браузере.

После просмотра устройств, которым назначен тег, вы можете создать и назначить новый тег или назначить существующий тег другим устройствам. В этом случае вам придется удалить фильтр по тегу, выбрать устройства и назначить тег.

Просмотр тегов, назначенных устройству

Чтобы просмотреть теги, назначенные устройству:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.

2. Выберите устройство, теги которого требуется просмотреть.

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

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

В панели инструментов можно выполнить следующие действия:

- Назначить устройству другой тег.
- Удалить уже назначенный тег.
- Просмотреть все теги устройств, которые существуют на Сервере администрирования.

Вы не можете просматривать назначенные теги локально на устройстве.

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 приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.
2. Выберите устройство, теги которого требуется просмотреть.
3. В открывшемся окне свойств устройства выберите вкладку **Теги**.
4. Установите флажок напротив тега, который требуется снять.

5. В верхней части списка нажмите на кнопку **Отменить назначение тега**.
6. В появившемся окне нажмите на кнопку **ОК**.

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 приложениями или Агентом администрирования. Для того чтобы управлять этими тегами, используйте утилиту klscflag.

Просмотр правил автоматического назначения тегов устройствам

Чтобы просмотреть правила автоматического назначения тегов устройствам,

Выполните одно из следующих действий:

- В главном окне приложения перейдите в раздел **Хранилища** → **Теги устройств** → **Правила автоматического назначения тегов**.
- Перейдите к просмотру тегов, назначенных устройству, а затем нажмите на кнопку **Настроить правила автоматического назначения тегов**.

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 может содержать не более 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 Linux, настроена сортировка с учетом регистра, учитывайте регистр при указании DNS-имени устройства. Иначе правила автоматического назначения тегов не будет работать.

   - **Приложения** – наличие на устройстве Агента администрирования, тип, версия, архитектура операционной системы и менеджер пакетов.
   - **Виртуальные машины** – принадлежность устройства к определенному типу виртуальных машин.
   - **Реестр приложений** – наличие на устройстве приложений различных производителей.
   - **Пользовательские параметры** – наличие на Android-устройстве значений пользовательских параметров или их соответствие заданным требованиям. Подробная информация об использовании пользовательских параметров представлена в справке Kaspersky Secure Mobility Management.

     Использование пользовательских параметров доступно только при установленном плагине Kaspersky Mobile Devices Protection and Management 10.59.4.32 или выше.

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 **ОК**.

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 "[\"TAG 1\",\"TAG 2\",\"TAG 3\"]" -
     svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     где `[\"TAG 1\",\"TAG 2\",\"TAG 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 "[\"NEW TAG\",\"TAG 1\",\"TAG
     2\",\"TAG 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     где `NEW TAG` – это тег, который вы хотите назначить устройству, `TAG 1`, `TAG 2`, `TAG 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 `TAG 1`, `TAG 2`, `TAG 3` – ваши текущие теги и вы хотите удалить `TAG 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 "[\"TAG 1\",\"TAG 3\"]" -svt ARRAY_T
     -ss "|ss_type = \"SS_PRODINFO\";"
     ```

3. Выполните следующую команду, чтобы перезапустить службу Агента администрирования:

   ```
   systemctl restart klnagent
   ```

   Утилита klscflag назначит вашему устройству указанные теги.

4. Если вы хотите убедиться, что утилита klscflag успешно назначила указанные теги, просмотрите теги, которые были назначены устройству.

Также можно назначать теги устройств вручную.

Шифрование и защита данных

Шифрование данных снижает риски непреднамеренной утечки информации в случае кражи/утери портативного устройства или жесткого диска. Также шифрование данных предотвращает доступ к данным неавторизованных пользователей и приложений.

Вы можете использовать функцию шифрования данных, если в вашей сети есть управляемые устройства с операционной системой Windows, на которых установлено приложение Kaspersky Endpoint Security для Windows. В этом случае на устройствах под управлением операционной системы Windows вы можете управлять следующими типами шифрования:

- шифрование диска BitLocker;
- шифрование диска Kaspersky.

Не рекомендуется включать шифрование в VDI.

С помощью этих компонентов Kaspersky Endpoint Security для Windows вы можете, например, включать или выключать шифрование, просматривать список зашифрованных жестких дисков, формировать и просматривать отчеты о шифровании.

Чтобы настроить шифрование, настройте политику Kaspersky Endpoint Security для Windows в Kaspersky Security Center Linux. Kaspersky Endpoint Security для Windows выполняет шифрование и расшифровку в соответствии с активной политикой. Подробные инструкции по настройке правил и описание особенностей шифрования см. в онлайн-справке Kaspersky Endpoint Security для Windows.

Управление шифрованием для иерархии Серверов администрирования в настоящее время недоступно в Web Console. Используйте главный Сервер администрирования для управления зашифрованными устройствами.

Вы можете отобразить или скрыть некоторые элементы интерфейса, связанные с управлением шифрованием, с помощью параметров пользовательского интерфейса.

Просмотр списка зашифрованных жестких дисков

В Kaspersky Security Center Linux вы можете просмотреть информацию о зашифрованных жестких дисках и об устройствах, зашифрованных на уровне дисков. После того, как информация на диске будет расшифрована, диск будет автоматически удален из списка.

Чтобы просмотреть список зашифрованных жестких дисков,

В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных** → **Зашифрованные жесткие диски**.

Если раздела нет в меню, значит, он скрыт. В настройках пользовательского интерфейса включите параметр **Показать раздел "Шифрование и защита данных"** для отображения раздела.

Вы можете экспортировать список зашифрованных жестких дисков в файлы форматов CSV или TXT. Для этого нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**.

Просмотр списка событий шифрования

В процессе выполнения задач шифрования или расшифровки данных на устройствах Kaspersky Endpoint Security для Windows отправляет в Kaspersky Security Center Linux информацию о возникающих событиях следующих типов:

- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за нехватки места на диске;
- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за проблем с лицензией;
- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за отсутствия прав доступа;
- приложению запрещен доступ к зашифрованному файлу;
- неизвестные ошибки.

Чтобы просмотреть список событий, возникших при шифровании данных на устройствах:

В главном окне приложения перейдите в раздел **Операции → Шифрование и защита данных → События шифрования**.

Если раздела нет в меню, значит, он скрыт. В настройках пользовательского интерфейса включите параметр **Показать раздел "Шифрование и защита данных"** для отображения раздела.

Вы можете экспортировать список зашифрованных жестких дисков в файлы форматов CSV или TXT. Для этого нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**.

Также можно просмотреть список событий шифрования для каждого управляемого устройства.

Чтобы просмотреть события шифрования управляемого устройства:

1. В главном окне приложения перейдите в раздел **Управление активами → Управляемые устройства**.
2. Нажмите на имя управляемого устройства.
3. На вкладке **Общие** перейдите в раздел **Защита**.
4. Перейдите по ссылке **Просмотреть ошибки шифрования данных**.

Формирование и просмотр отчетов о шифровании

Вы можете формировать следующие отчеты:

- Отчет о статусе шифрования управляемых устройств. В этом отчете представлены сведения о шифровании данных различных управляемых устройств. Например, в отчете показано количество устройств, к которым применяется политика с настроенными правилами шифрования. Также можно узнать, например, сколько устройств нужно перезагрузить. Отчет также содержит информацию о технологии и алгоритме шифрования для каждого устройства.

- Отчет о статусе шифрования запоминающих устройств. Этот отчет содержит похожую информацию, что и отчет о состоянии шифрования управляемых устройств, но предоставляет данные только для запоминающих устройств и съемных дисков.

- Отчет о правах доступа к зашифрованным жестким дискам. Этот отчет показывает, какие учетные записи пользователей имеют доступ к зашифрованным жестким дискам.

- Отчет об ошибках шифрования файлов. Отчет содержит информацию об ошибках, которые возникли при выполнении задач шифрования или расшифровки данных на устройствах.

- Отчет о блокировании доступа к зашифрованным файлам. Отчет содержит информацию о блокировке доступа приложений к зашифрованным файлам. Этот отчет полезен, если неавторизованный пользователь или приложение пытается получить доступ к зашифрованным файлам или жестким дискам.

Вы можете сгенерировать любой отчет в разделе **Мониторинг** → **Отчеты**. Также в разделе **Операции** → **Шифрование и защита данных**, можно создавать следующие отчеты о шифровании:

- Отчет о статусе шифрования запоминающих устройств

- Отчет о правах доступа к зашифрованным жестким дискам

- Отчет об ошибках шифрования файлов

*Чтобы сгенерировать отчет шифрования в разделе **Шифрование и защита данных**:*

1. Убедитесь, что параметр **Показать раздел "Шифрование и защита данных"** в параметрах интерфейса включен.

2. В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных**.

3. Откройте один из следующих разделов:

   - **Зашифрованные жесткие диски** – формирует отчет о состоянии шифрования запоминающих устройств или отчет о правах доступа к зашифрованным жестким дискам.

   - **События шифрования** – формирует отчет об ошибках шифрования файлов.

4. Выберите название отчета, который требуется сгенерировать.

Запустится процесс формирования отчета.

Предоставление доступа к зашифрованному жесткому диску в автономном режиме

Пользователь может запросить доступ к зашифрованному устройству, например, если Kaspersky Endpoint Security не установлен на управляемом устройстве. После получения запроса вы можете создать файл ключа доступа и отправить его пользователю. Все варианты использования и подробные инструкции приведены в справке Kaspersky Endpoint Security для соответствующей платформы.

Порядок предоставления доступа к зашифрованному жесткому диску в автономном режиме в Kaspersky Endpoint Security для Windows:

1. Получите файл запроса доступа от пользователя (файл с расширением FDERTC). Следуйте инструкциям в онлайн-справке Kaspersky Endpoint Security для Windows, чтобы сгенерировать файл в Kaspersky Endpoint Security для Windows.

2. В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных** → **Зашифрованные жесткие диски**.

   Отобразится список зашифрованных жестких дисков.

3. Выберите диск, к которому пользователь запросил доступ.

4. Нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.

5. В открывшемся окне выберите плагин Kaspersky Endpoint Security для Windows.

6. Следуйте инструкциям, приведенным в онлайн-справке Kaspersky Endpoint Security для Windows (см. инструкции для Kaspersky Security Center Web Console в конце раздела).

После этого пользователь может использовать полученный файл для доступа к зашифрованному жесткому диску и чтения данных, хранящихся на диске.

Передача ключей шифрования между Серверами администрирования

Если на управляемом устройстве включена функция шифрования данных, ключ шифрования хранится на Сервере администрирования. Ключ шифрования используется для доступа к зашифрованным данным и для управления политикой шифрования.

Ключ шифрования должен быть передан на другой Сервер администрирования в следующих случаях:

- Перенастройка Агента администрирования на управляемом устройстве для назначения устройства другому Серверу администрирования. Если это устройство содержит зашифрованные данные, ключ шифрования должен быть передан на целевой Сервер администрирования. В противном случае не удастся расшифровать данные.

- Шифрование съемного диска, подключенного к устройству D1, которым управляет Сервер администрирования S1, и затем подключение этого съемного диска к устройству D2, управляемому Сервером администрирования S2. Для доступа к данным на съемном диске ключ шифрования должен быть передан с Сервера администрирования S1 на Сервер администрирования S2.

- Шифрование файла на устройстве D1, управляемом Сервером администрирования S1, и затем попытка получить доступ к файлу на устройстве D2, управляемом Сервером администрирования S2. Для доступа к файлу ключ шифрования должен быть передан с Сервера администрирования S1 на Сервер администрирования S2.

Ключи шифрования можно передавать следующими способами:

- Автоматически, включив параметр **Использовать иерархию Серверов администрирования для получения ключей шифрования** в свойствах двух Серверов администрирования, между которыми должен передаваться ключ шифрования. Если этот параметр выключен для одного из Серверов администрирования, автоматическая передача ключей шифрования невозможна.

  При включении параметра **Использовать иерархию Серверов администрирования для получения ключей шифрования** в свойствах Сервера администрирования, Сервер администрирования отправляет ключи шифрования на главный Сервер администрирования (если он существует) на один уровень иерархии выше.

  Когда вы пытаетесь получить доступ к зашифрованным данным, Сервер администрирования сначала ищет ключ шифрования в своем хранилище. Если включен параметр **Использовать иерархию Серверов администрирования для получения ключей шифрования**, а требуемый ключ шифрования отсутствует в хранилище, Сервер администрирования дополнительно отправляет запрос на главный Сервер администрирования (если он существует), чтобы получить требуемый ключ шифрования. Запрос отправляется на все главные Серверы администрирования, вплоть до Сервера на самом верхнем уровне иерархии.

- Вручную от одного Сервера администрирования другому путем экспорта и импорта файла, содержащего ключи шифрования.

  Экспорт и импорт ключей шифрования – это действия, включенные в функционал управления ключами шифрования. Чтобы выполнить эти действия, настройте права доступа к функции для пользователей Kaspersky Security Center Linux следующим образом:

  - Предоставить право **Чтение** к функции Управление ключами шифрования для пользователя, который экспортирует ключи шифрования с подчиненного Сервера администрирования.

  - Предоставить право **Запись** к функции Управление ключами шифрования для пользователя, импортирующего ключи шифрования на требуемый Сервер администрирования.

Чтобы включить автоматическую передачу ключей шифрования между Серверами администрирования в иерархии:

1. Перейдите в свойства нужного Сервера администрирования:

   a. В главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**.

   b. В открывшейся панели наведите курсор мыши на название нужного Сервера администрирования и нажмите на значок параметров (⚙).

      Вы также можете нажать на имя Сервера администрирования, а после того как имя отобразится в главном меню, нажать на него в главном меню, чтобы открыть окно свойств Сервера.

2. В открывшемся окне свойств выберите раздел **Алгоритм шифрования**.

3. Включите параметр **Использовать иерархию Серверов администрирования для получения ключей шифрования**.

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

Ключи шифрования будут переданы на главный Сервер администрирования (если он существует) при следующей синхронизации (пакете пульса). Этот Сервер администрирования также предоставляет по запросу ключ шифрования от своего хранилища подчиненному Серверу администрирования.

Чтобы передать ключи шифрования между Серверами администрирования вручную:

1. Перейдите в свойства Сервера администрирования, с которого вы хотите экспортировать ключи шифрования:

   a. В главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**.

   b. В открывшейся панели наведите курсор мыши на название нужного Сервера администрирования и нажмите на значок параметров (⚙).

      Вы также можете нажать на имя Сервера администрирования, а после того как имя отобразится в главном меню, нажать на него в главном меню, чтобы открыть окно свойств Сервера.

2. В открывшемся окне свойств выберите раздел **Алгоритм шифрования**.

3. Нажмите на кнопку **Экспорт ключей шифрования**.

   Убедитесь, что пользователю, который экспортирует ключи шифрования с Сервера, предоставлено право **Чтение** к функции Управления ключами шифрования.

4. В окне **Экспортировать ключи шифрования с Сервера администрирования?** выполните следующие действия:

   a. Укажите пароль, чтобы защитить файл от несанкционированного доступа.

   b. Укажите, куда сохранить файл.

> Запомните пароль. Утерянный пароль не может быть восстановлен. Если пароль утерян, необходимо повторить процедуру экспорта. Поэтому запишите пароль и держите его под рукой.

5. Передайте файл на другой Сервер администрирования, например, с помощью папки общего доступа или съемного диска.

6. Перейдите в свойства Сервера администрирования, на который вы хотите импортировать ключи шифрования.

7. В окне свойств выберите раздел **Алгоритм шифрования**.

8. Нажмите на кнопку **Импорт ключей шифрования**.

   Убедитесь, что пользователю, импортирующему ключи шифрования на Сервер, предоставлено право **Запись** к функции Управления ключами шифрования.

9. Выберите файл, содержащий ключи шифрования.

10. Укажите пароль и нажмите на кнопку **OK**.

Ключи шифрования будут переданы на целевой Сервер администрирования.

Смена Сервера администрирования для клиентских устройств

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 создания задачи **Новая задача** выберите приложение **Kaspersky Security Center 17** 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 определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

- **Назначить задачу выборке устройств**

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

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

3. Запустите созданную задачу.

После завершения работы задачи клиентские устройства, для которых она была создана, переходят под управление Сервера администрирования, указанного в параметрах задачи.

Если Сервер администрирования поддерживает управление шифрованием и защитой данных, то при создании задачи *Смена Сервера администрирования* отображается предупреждение. Предупреждение содержит информацию о том, что при наличии на устройствах зашифрованных данных после переключения устройств под управлением другого Сервера пользователям будет предоставлен доступ только к тем зашифрованным данным, с которыми они работали ранее. В остальных случаях доступ к зашифрованным данным предоставлен не будет. Подробное описание сценариев, в которых доступ к зашифрованным данным не будет предоставлен, приведено в справке Kaspersky Endpoint Security для Windows.

Избегание конфликтов между Серверами администрирования

Если в сети имеется несколько Серверов администрирования, они могут видеть одни и те же клиентские устройства. Это может привести к тому, что, например, Сервер администрирования установит приложение, которое уже было установлено другим Сервером, а также к другим конфликтам. Чтобы запретить установку приложения на устройство, управляемое другим Сервером администрирования, нужно включить параметр **Устанавливать на устройства, управляемые только этим Сервером администрирования** в свойствах задачи *Удаленная установка приложения*.

Если вы включите параметр **Устанавливать на устройства, управляемые только этим Сервером администрирования** и запустите задачу *Удаленная установка приложения*, выполнится проверка для определения, находятся ли устройства под управлением другого Сервера администрирования. Для устройств, управляемых другим Сервером администрирования, для атрибута **Под управлением другого Сервера администрирования** будет установлено значение `true`. Задача *Удаленная установка приложения* к этим устройствам не применяется.

Значения атрибута **Под управлением другого Сервера администрирования** отображаются в столбце **Под управлением другого Сервера администрирования** в списке управляемых устройств и в списке нераспределенных устройств.

Свойство **Под управлением другого Сервера администрирования** можно также использовать как критерий для следующих операций:

- Отображение управляемых устройств.
- Выборки устройств.

- Правила перемещения устройств.
- Правила автоматического назначения тегов.

Чтобы сбросить атрибут Под управлением другого Сервера администрирования:

1. В главном меню Kaspersky Security Center Web Console перейдите в раздел **Управление активами** → **Нераспределенные устройства**.
2. Выберите нужное устройство и нажмите на кнопку **Удалить атрибут "Управляется другим Сервером администрирования"**.

Атрибут **Под управлением другого Сервера администрирования** будет сброшен.

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 <Server address>`, 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 "<Connection gateway IP address or name>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     Здесь `<Connection gateway IP address 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

Если клиентские устройства группы администрирования неактивны, вы можете получать уведомления об этом. Вы также можете автоматически удалять такие устройства.

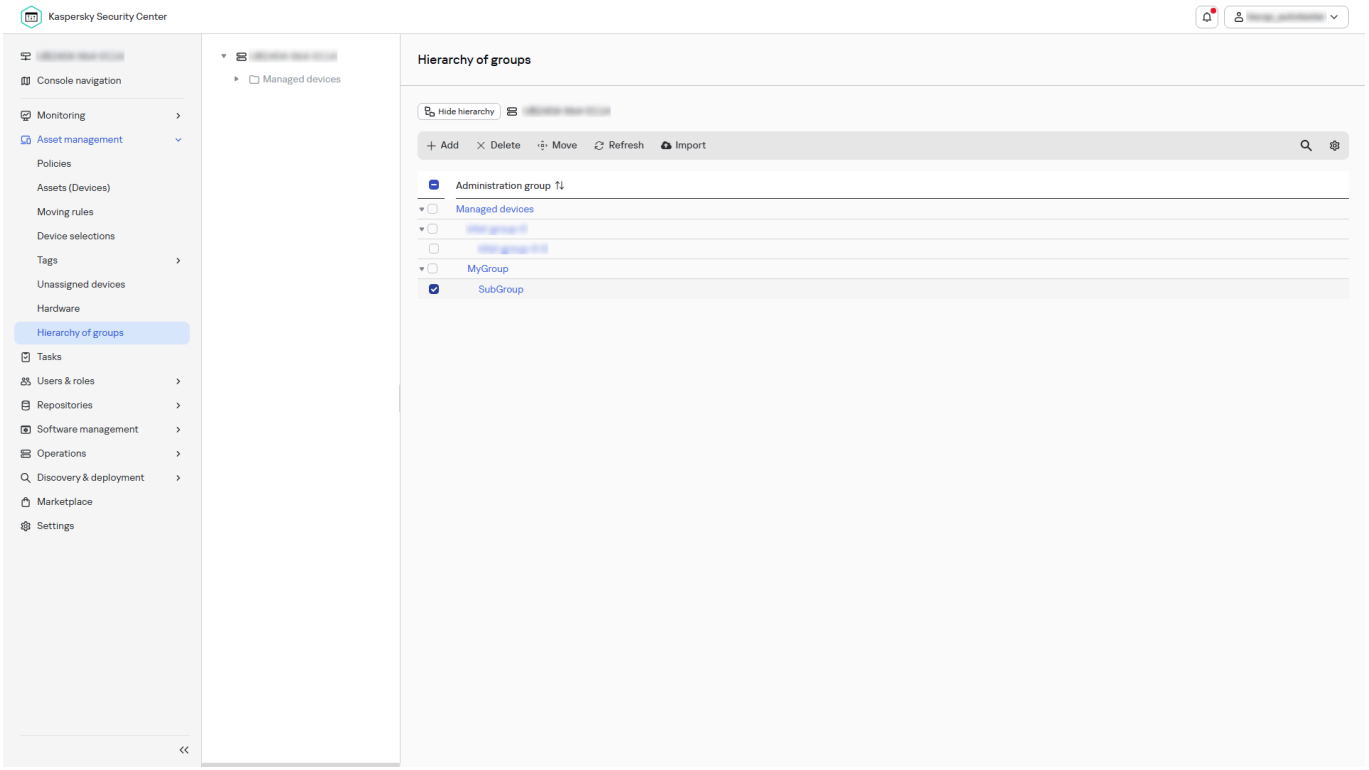
Чтобы просмотреть или настроить действия, когда устройства неактивны в группе администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп**.

2. Перейдите к свойствам нужной группы администрирования одним из следующих способов:

   - Выберите имя группы администрирования.

   - Нажмите на кнопку **Показать иерархию** в верхней части страницы. В открывшейся панели наведите курсор мыши на название нужной группы и нажмите на значок параметров (⚙).



Иерархия групп администрирования

Откроется окно свойств группы администрирования.

3. В окне свойств перейдите на вкладку **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.

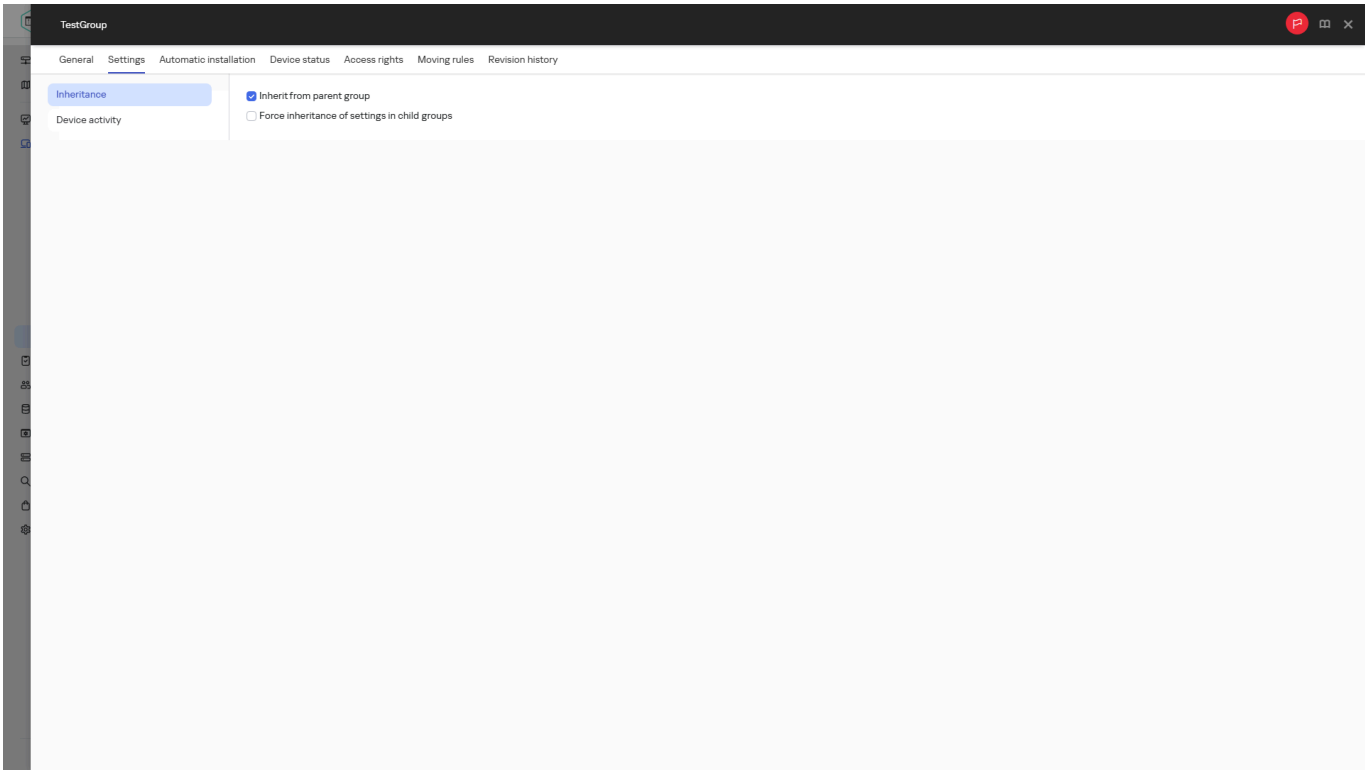
   Этот параметр доступен только для группы администрирования, у которой есть родительская группа администрирования.

   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.



Свойства группы администрирования

5. В разделе **Активность устройств** включите или выключите следующие параметры:

   Уведомлять администратора, если устройство неактивно больше (сут)

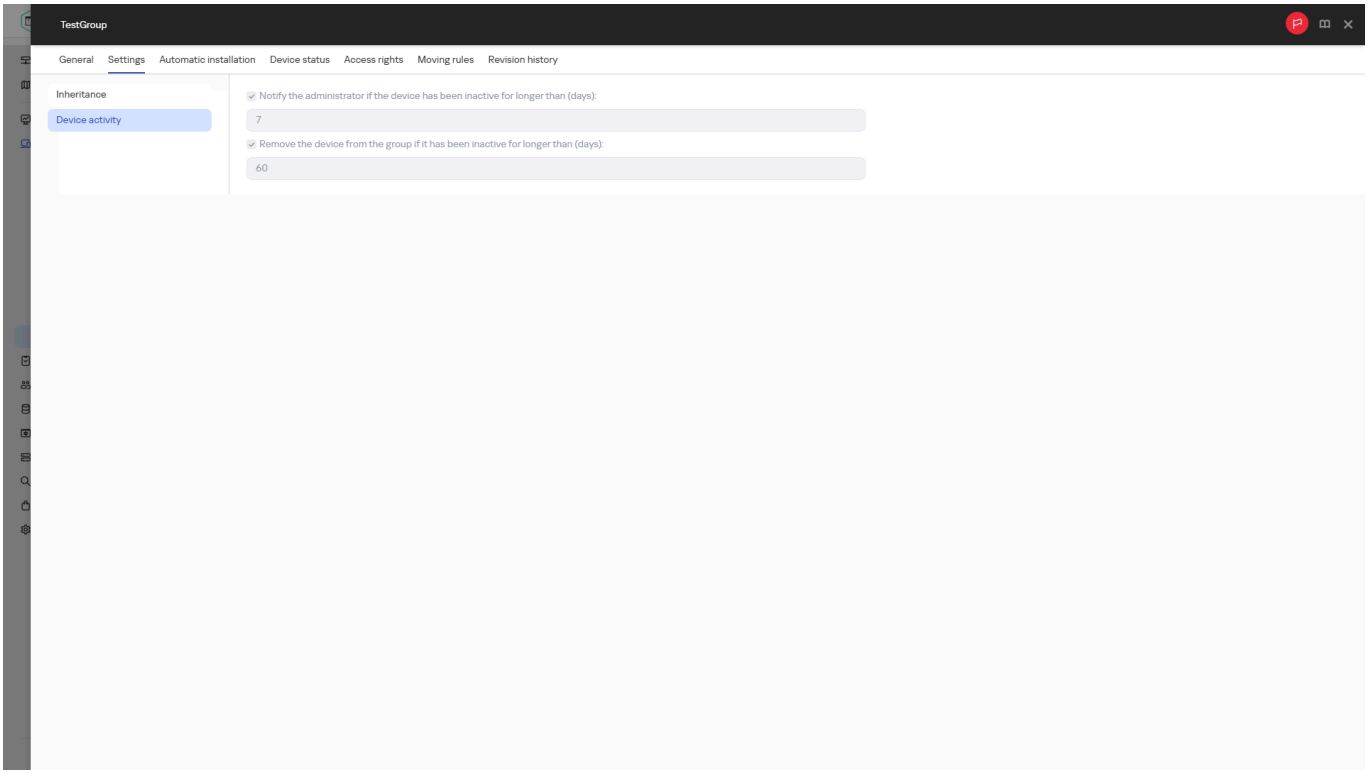
   Если этот параметр включен, администратор получает уведомления о неактивности устройств. В поле ввода можно задать интервал времени, по истечении которого будет сформировано событие **Устройство долго не проявляет активности в сети**. Временной интервал, установленный по умолчанию, составляет 7 дней.

   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.



Свойства группы администрирования

6. Нажмите на кнопку **Сохранить**.

Ваши изменения сохранены и применены.

Отправка сообщения пользователям устройств

Чтобы отправить сообщение пользователям устройств:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В раскрывающемся списке **Тип задачи** выберите **Сообщение для пользователя**.
4. Выберите параметр, чтобы указать группу администрирования, выборку устройств или устройства, к которым применяется задача.
5. Запустите созданную задачу.

После завершения работы задачи созданное сообщение будет отправлено пользователям выбранных устройств. Задача **Сообщение для пользователя** доступна только для устройств под управлением операционной системы Windows.

Удаленное включение, выключение и перезагрузка клиентских устройств

Kaspersky Security Center Linux позволяет удаленно управлять клиентскими устройствами, включать, выключать и перезагружать их.

Чтобы удаленно управлять клиентскими устройствами:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В раскрывающемся списке **Тип задачи** выберите **Управление устройствами**.
4. Выберите параметр, чтобы указать группу администрирования, выборку устройств или устройства, к которым применяется задача.
5. Выберите команду (включить, выключить или перезагрузить).
6. При необходимости настройте следующие параметры для команд выключения и перезагрузки:

   - Включите переключатель **Запрашивать подтверждение у пользователя**, чтобы указать сообщение для запроса у пользователя и период повтора запроса, а также повторного запуска перезагрузки или выключения устройства.
   - Установите флажок **Время ожидания перед принудительным закрытием приложения в заблокированных сеансах через (мин)** и укажите время.

   Эти параметры применимы только к клиентским устройствам с операционной системой Windows. Устройства с операционной системой Linux будут перезагружены или выключены сразу после завершения задачи.
7. Запустите созданную задачу.

После завершения работы задачи команда (включение, выключение или перезагрузка) будет выполнена на выбранных устройствах.

Удаленный доступ к управляемым устройствам

Kaspersky Security Center Linux позволяет устанавливать удаленное подключение к управляемым устройствам. Вы можете получить удаленный доступ к управляемому устройству с помощью Агента администрирования, установленного на устройстве. Удаленное подключение к клиентскому устройству с помощью Агента администрирования возможно и в том случае, если TCP- и UDP-порты клиентского устройства закрыты для доступа. После подключения к устройству администратор получает полный доступ к информации на этом устройстве и может управлять приложениями, установленными на нем.

Способы установки удаленного подключения зависят от того, какая платформа используется на устройстве с Kaspersky Security Center Web Console. Приложение Kaspersky Security Center Web Console может быть установлено на устройство с операционной системой Windows или Linux, отличное от устройства Сервера администрирования.

От приложения Kaspersky Security Center Web Console, установленного на устройстве с операционной системой Linux, вы можете установить следующие подключения:

- К управляемому устройству с операционной системой Linux с помощью:
  - Удаленное подключение к рабочему столу (Remote desktop connection, RDP).
  - Virtual Network Computing (VNC).
- К управляемому устройству с операционной системой Windows с помощью:
  - Удаленное подключение к рабочему столу (Remote desktop connection, RDP).
  - Virtual Network Computing (VNC).

От приложения Kaspersky Security Center Web Console, установленного на устройстве с операционной системой Windows, вы можете установить следующие подключения:

- К управляемому устройству с операционной системой Linux с помощью:
  - Удаленное подключение к рабочему столу (Remote desktop connection, RDP).
  - Virtual Network Computing (VNC).
- К управляемому устройству с операционной системой Windows с помощью:
  - Удаленное подключение к рабочему столу (Remote desktop connection, RDP).
  - Совместный доступ к рабочему столу (Windows Desktop Sharing, WDS).

Удаленное подключение к управляемым устройствам не поддерживается при доступе к Kaspersky Security Center Web Console с устройства с операционной системой Microsoft Windows на Arm.

Чтобы установить удаленное подключение с устройством, у вам потребуется следующее:

- Утилита klsctunnel.

  Утилита "Лаборатории Касперского" используется для туннелирования соединения между управляемым устройством и Сервером администрирования.

  Kaspersky Security Center Linux позволяет туннелировать TCP-соединения от Kaspersky Security Center Web Console через Сервер администрирования и далее через Агент администрирования к заданному порту на управляемом устройстве. Туннелирование используется для подключения клиентского приложения, находящегося на устройстве с установленным приложением Kaspersky Security Center Web Console, к TCP-порту на управляемом устройстве, если прямое соединение устройства с Kaspersky Security Center Web Console с устройством невозможно.

Туннелирование соединения удаленного клиентского устройства с Сервером администрирования необходимо, если на устройстве недоступен порт для соединения с Сервером администрирования. Порт на устройстве может быть недоступен в следующих случаях:

- Удаленное устройство подключено к локальной сети, в которой используется механизм NAT.
- Удаленное устройство входит в локальную сеть Сервера администрирования, но его порт закрыт сетевым экраном.

Вы можете скачать утилиту из Kaspersky Security Center Web Console, если удаленное подключение установлено с помощью Web Console, или вручную с сайта "Лаборатории Касперского".

Утилита klsctunnel установлена на устройстве Сервера администрирования и используется для всех типов удаленного подключения (RDP, VNC, WDS).

- RDP- или VNC-клиент.

  RDP- или VNC-клиент установлен на устройстве Сервера администрирования. Этот клиент позволяет вам получить удаленный доступ к управляемому устройству, используя адрес и порт для локального подключения, предоставленные утилитой klsctunnel.

  RDP-подключение к существующему сеансу удаленного рабочего стола пользователя осуществляется без уведомления пользователя. Как только вы подключаетесь к сеансу, пользователь устройства автоматически отключается от сеанса без получения уведомления.

- Совместный доступ к рабочему столу Windows (только для управляемых устройств с операционной системой Windows)

  Эта функция позволяет вам подключиться к существующему сеансу на клиентском устройстве, не отключая пользователя, работающего в этом сеансе. В этом случае у администратора и пользователя сеанса на устройстве есть совместный доступ к рабочему столу.

  При подключении к существующему сеансу удаленного рабочего стола пользователь этого сеанса на устройстве получит запрос от администратора на подключение. Информация о процессе удаленной работы с устройством и результатах этой работы не сохраняется в отчетах Kaspersky Security Center Linux.

  Администратор может настроить аудит действий на удаленном клиентском устройстве. В ходе аудита приложение сохраняет информацию о файлах на клиентском устройстве, которые открывал и/или изменял администратор.

Удаленный доступ с Linux-устройства с Kaspersky Security Center Web Console к управляемому Linux-устройству

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- На управляемом устройстве с операционной системой Linux установлен Агент администрирования версии 15.3 или выше.
- На управляемом устройстве с операционной системой Linux установлен RDP-сервер (если вы подключаетесь к управляемому устройству с использованием Remote Desktop Connection).

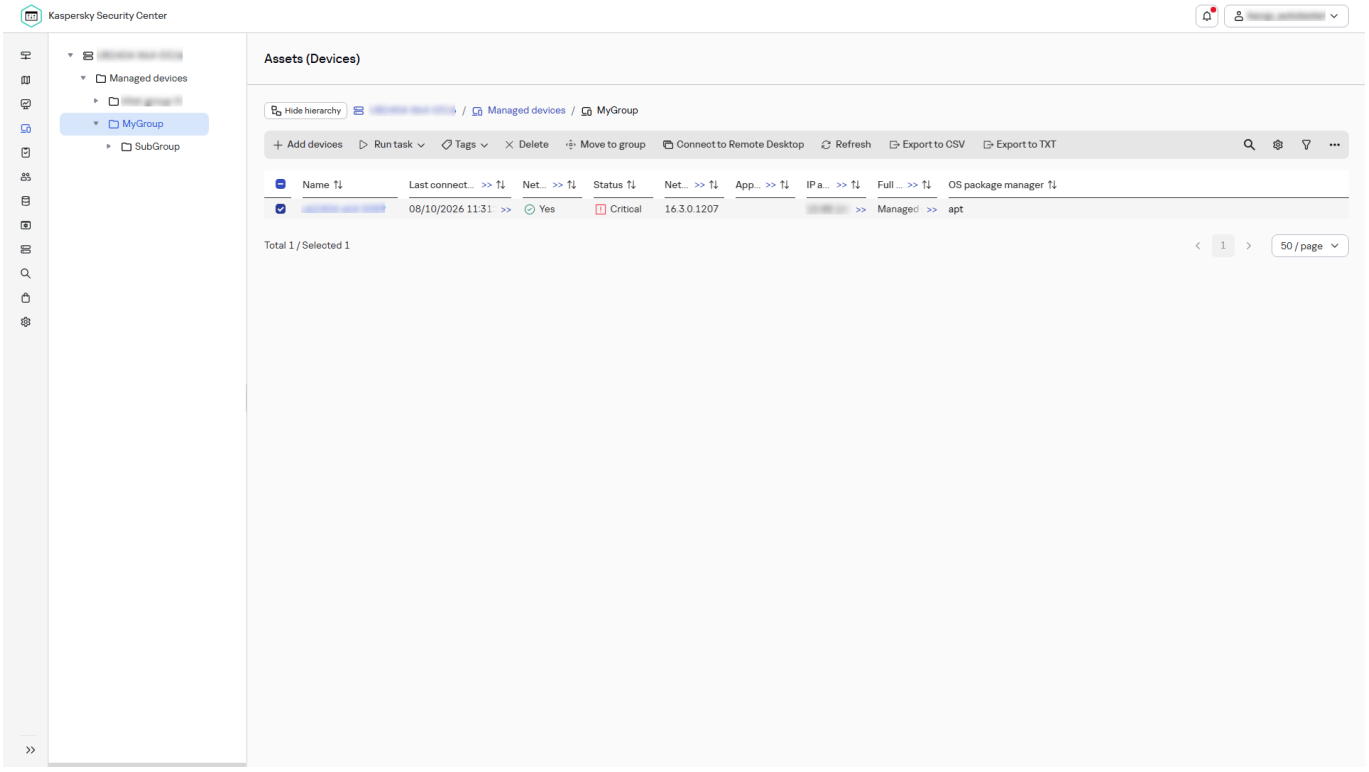
- На управляемом устройстве с операционной системой Linux установлен VNC-сервер (если вы подключаетесь к управляемому устройству с использованием Virtual Network Computing).
- Порт для туннелирования RDP-соединений открыт (в окне свойств Сервера администрирования в разделе **Порты подключения** включен параметр **Открыть порт для туннельного RDP-подключения**).
- У администратора есть право **Запуск RDP-сеансов** для установки RDP-соединений (если вы подключаетесь к управляемому устройству с помощью Remote Desktop Connection).
- У администратора есть право **Создание туннелирования** для установки туннельного соединения для VNC (если вы подключаетесь к управляемому устройству с помощью Virtual Network Computing).

Чтобы подключиться к управляемому устройству с операционной системой Linux по RDP или VNC с помощью приложения Kaspersky Security Center Web Console, которое открыто на устройстве с операционной системой Linux:

1. В главном меню перейдите в раздел **Управление активами** → **Управляемые устройства** или откройте выборку устройств.
2. Установите флажок рядом с управляемым устройством, к которому вы хотите подключиться удаленно и нажмите на кнопку **Подключиться к удаленному рабочему столу**.

   Откроется окно **Подключиться к удаленному рабочему столу**.

   Если вы выберете несколько устройств, мобильное устройство или устройство с операционной системой macOS, кнопка **Подключиться к удаленному рабочему столу** будет неактивна.



Список управляемых устройств

3. Скачайте утилиту klsctunnel, нажав на кнопку **Скачать**, и запустите ее.

При скачивании утилиты учитывайте следующее:

- Чтобы получить актуальную версию утилиты klsctunnel убедитесь, что Сервер администрирования имеет доступ к серверам обновлений "Лаборатории Касперского".

  Вы можете запустить задачу *Загрузка обновлений в хранилище Сервера администрирования* и выбрать серверы обновлений "Лаборатории Касперского" в качестве источника обновлений. Если задача завершается успешно, Сервер администрирования имеет доступ к серверам обновлений "Лаборатории Касперского".

- Если файл утилиты недоступен для скачивания, отображается сообщение об ошибке. В этом случае скачайте утилиту вручную и поместите ее на устройство, на котором установлен Сервер администрирования, в директорию /var/opt/kaspersky/klnagent_srv.

4. В окне **Подключиться к удаленному рабочему столу** укажите порт подключения. По умолчанию номер порта – 3389.

5. Создайте текстовый BLOB-объект с зашифрованными параметрами подключения, нажав на кнопку **Сгенерируйте BLOB-объект**, скопируйте и вставьте текст в соответствующее поле в утилите klsctunnel.

   BLOB-объект содержит параметры, необходимые для установки соединения между Сервером администрирования и управляемым устройством. BLOB-объект действителен в течение трех минут. Если срок его действия истек, сгенерируйте BLOB-объект повторно.

6. Если вы используете прокси-сервер, в утилите klsctunnel укажите параметры подключения к прокси-серверу.

   Утилита klsctunnel отображает адрес и порт для локального подключения клиента удаленного доступа.

   Утилита позволяет администратору закрыть туннельное соединение. Если туннельное соединение закрыто, текущее соединение с удаленным рабочим столом прекращается.

7. Запустите клиент удаленного доступа (RDP или VNC) и подключите его к управляемому устройству, используя адрес и порт, предоставленные утилитой klsctunnel.

Соединение с управляемым устройством установлено. Рабочий стол доступен в окне клиента удаленного доступа.

Удаленный доступ с Linux-устройства с Kaspersky Security Center Web Console к управляемому Windows-устройству

Удаленное подключение к рабочему столу (Remote desktop connection, RDP).

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- Удаленное подключение разрешено в параметрах операционной системы управляемого устройства.

- На управляемом устройстве с операционной системой Windows установлен Агент администрирования версии 13 или выше.

- У администратора есть право **Запуск RDP-сеансов** для установления RDP-соединений.
- Порт для туннелирования RDP-соединений открыт (в окне свойств Сервера администрирования в разделе **Порты подключения** включен параметр **Открыть порт для туннельного RDP-подключения**).

Чтобы подключиться к управляемому устройству с операционной системой Windows по RDP с помощью приложения Kaspersky Security Center Web Console, которое открыто на устройстве с операционной системой Linux:

1. В главном меню перейдите в раздел **Управление активами** → **Управляемые устройства** или откройте выборку устройств.
2. Установите флажок рядом с управляемым устройством, к которому вы хотите подключиться удаленно и нажмите на кнопку **Подключиться к удаленному рабочему столу**.

   Откроется окно **Подключиться к удаленному рабочему столу**.

   Если вы выберете несколько устройств, мобильное устройство или устройство с операционной системой macOS, кнопка **Подключиться к удаленному рабочему столу** будет неактивна.
3. В окне **Подключиться к удаленному рабочему столу** выберите тип подключения **RDP**.
4. Если удаленное подключение не разрешено в параметрах операционной системы управляемого устройства, разрешите удаленное подключение централизованно, нажав на кнопку **Изменить параметры**.

   Если параметры применены правильно, отображается уведомление. Также на управляемом устройстве в разделе **Параметры** → **Система** → **Удаленный рабочий стол** должен быть включен параметр **Включить удаленный рабочий стол**.

   Если удаленное подключение разрешено в параметрах операционной системы управляемого устройства, кнопка **Изменить параметры** не отображается.
5. Скачайте утилиту klsctunnel, нажав на кнопку **Скачать**, и запустите ее.

   При скачивании утилиты учитывайте следующее:

   - Чтобы получить актуальную версию утилиты klsctunnel убедитесь, что Сервер администрирования имеет доступ к серверам обновлений "Лаборатории Касперского".

     Вы можете запустить задачу *Загрузка обновлений в хранилище Сервера администрирования* и выбрать серверы обновлений "Лаборатории Касперского" в качестве источника обновлений. Если задача завершается успешно, Сервер администрирования имеет доступ к серверам обновлений "Лаборатории Касперского".
   - Если файл утилиты недоступен для скачивания, отображается сообщение об ошибке. В этом случае скачайте утилиту вручную и поместите ее на устройство, на котором установлен Сервер администрирования, в директорию /var/opt/kaspersky/klnagent_srv.
6. Создайте текстовый BLOB-объект с зашифрованными параметрами подключения, нажав на кнопку **Сгенерируйте BLOB-объект**, скопируйте и вставьте текст в соответствующее поле в утилите klsctunnel.

   BLOB-объект содержит параметры, необходимые для установки соединения между Сервером администрирования и управляемым устройством. BLOB-объект действителен в течение трех минут. Если срок его действия истек, сгенерируйте BLOB-объект повторно.
7. Если вы используете прокси-сервер, в утилите klsctunnel укажите параметры подключения к прокси-серверу.

   Утилита klsctunnel отображает адрес и порт для локального подключения удаленного устройства.

Утилита позволяет администратору закрыть туннельное соединение. Если туннельное соединение закрыто, текущее соединение с удаленным рабочим столом прекращается.

8. Запустите RDP-клиент и подключите его к управляемому устройству, используя адрес и порт, предоставленные утилитой klsctunnel.

Соединение с управляемым устройством установлено. Рабочий стол доступен в окне RDP-клиента.

Подключение к существующему сеансу удаленного рабочего стола пользователя осуществляется без уведомления пользователя. Как только вы подключаетесь к сеансу, пользователь устройства автоматически отключается от сеанса без получения уведомления.

Система Virtual Network Computing (VNC)

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- На управляемом устройстве с операционной системой Windows установлен Агент администрирования версии 13 или выше.
- На управляемом устройстве с операционной системой Windows установлен VNC-сервер.
- У администратора есть право **Создание туннелирования** для установки туннельного соединения для VNC.
- Порт для туннелирования RDP-соединений открыт (в окне свойств Сервера администрирования в разделе **Порты подключения** включен параметр **Открыть порт для туннельного RDP-подключения**).

Чтобы подключиться к управляемому устройству с операционной системой Windows по VNC с помощью приложения Kaspersky Security Center Web Console, которое открыто на устройстве с операционной системой Linux:

1. В главном меню перейдите в раздел **Управление активами** → **Управляемые устройства** или откройте выборку устройств.
2. Установите флажок рядом с управляемым устройством, к которому вы хотите подключиться удаленно и нажмите на кнопку **Подключиться к удаленному рабочему столу**.

   Откроется окно **Подключиться к удаленному рабочему столу**.

   Если вы выберете несколько устройств, мобильное устройство или устройство с операционной системой macOS, кнопка **Подключиться к удаленному рабочему столу** будет неактивна.
3. В окне **Подключиться к удаленному рабочему столу** выберите тип подключения **VNC**.
4. Скачайте утилиту klsctunnel, нажав на кнопку **Скачать**, и запустите ее.

   Если файл утилиты недоступен для скачивания, отображается сообщение об ошибке. В этом случае скачайте утилиту вручную.
5. В окне **Подключиться к удаленному рабочему столу** укажите порт VNC-подключения. По умолчанию номер порта – 5900.

6. Создайте текстовый BLOB-объект с зашифрованными параметрами подключения, нажав на кнопку **Сгенерируйте BLOB-объект**, скопируйте и вставьте текст в соответствующее поле в утилите klsctunnel.

   BLOB-объект содержит параметры, необходимые для установки соединения между Сервером администрирования и управляемым устройством. BLOB-объект действителен в течение трех минут. Если срок его действия истек, сгенерируйте BLOB-объект повторно.

7. Если вы используете прокси-сервер, в утилите klsctunnel укажите параметры подключения к прокси-серверу.

   Утилита klsctunnel отображает адрес и порт для локального подключения VNC-клиента.

   Утилита позволяет удаленному пользователю закрыть туннельное соединение. Если туннельное соединение закрыто, текущее соединение с удаленным рабочим столом прекращается.

8. Запустите VNC-клиент и подключите его к управляемому устройству, используя адрес и порт, предоставленные утилитой klsctunnel.

Соединение с управляемым устройством установлено. Рабочий стол доступен в окне VNC-клиента.

Удаленный доступ с Windows-устройства с Kaspersky Security Center Web Console к управляемому Linux-устройству

Удаленное подключение к рабочему столу (Remote desktop connection, RDP).

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- На управляемом устройстве с операционной системой Linux установлен RDP-сервер.
- На управляемом устройстве с операционной системой Linux установлен Агент администрирования версии 15.3 или выше.
- У администратора есть право **Запуск RDP-сеансов** для установления RDP-соединений.
- Порт для туннелирования RDP-соединений открыт (в окне свойств Сервера администрирования в разделе **Порты подключения** включен параметр **Открыть порт для туннельного RDP-подключения**).

Чтобы подключиться к управляемому устройству с операционной системой Linux по RDP с помощью приложения Kaspersky Security Center Web Console, которое открыто на устройстве с операционной системой Windows:

1. В главном меню перейдите в раздел **Управление активами** → **Управляемые устройства** или откройте выборку устройств.

2. Установите флажок рядом с управляемым устройством, к которому вы хотите подключиться удаленно и нажмите на кнопку **Подключиться к удаленному рабочему столу**.

   Откроется окно **Подключиться к удаленному рабочему столу**.

   Если вы выберете несколько устройств, мобильное устройство или устройство с операционной системой macOS, кнопка **Подключиться к удаленному рабочему столу** будет неактивна.

3. В окне **Подключиться к удаленному рабочему столу** выберите тип подключения **RDP**.

4. Скачайте утилиту klsctunnel, нажав на кнопку **Скачать**, и запустите ее.

   При скачивании утилиты учитывайте следующее:

   - Чтобы получить актуальную версию утилиты klsctunnel убедитесь, что Сервер администрирования имеет доступ к серверам обновлений "Лаборатории Касперского".

     Вы можете запустить задачу *Загрузка обновлений в хранилище Сервера администрирования* и выбрать серверы обновлений "Лаборатории Касперского" в качестве источника обновлений. Если задача завершается успешно, Сервер администрирования имеет доступ к серверам обновлений "Лаборатории Касперского".

   - Если файл утилиты недоступен для скачивания, отображается сообщение об ошибке. В этом случае скачайте утилиту вручную и поместите ее на устройство, на котором установлен Сервер администрирования, в директорию /var/opt/kaspersky/klnagent_srv.

5. Создайте текстовый BLOB-объект с зашифрованными параметрами подключения, нажав на кнопку **Сгенерируйте BLOB-объект**, скопируйте и вставьте текст в соответствующее поле в утилите klsctunnel.

   BLOB-объект содержит параметры, необходимые для установки соединения между Сервером администрирования и управляемым устройством. BLOB-объект действителен в течение трех минут. Если срок его действия истек, сгенерируйте BLOB-объект повторно.

6. Если вы используете прокси-сервер, в утилите klsctunnel укажите параметры подключения к прокси-серверу.

   Для этого установите флажок **Использовать прокси-сервер** и укажите параметры подключения.

7. Нажмите на кнопку **Открыть порт**.

   Откроется окно входа в систему подключения к удаленному рабочему столу.

8. Укажите учетные данные учетной записи, под которой вы в настоящий момент входите в Kaspersky Security Center Web Console, и подключитесь к управляемому устройству.

   Утилита klsctunnel отображает адрес и порт для локального подключения удаленного устройства.

   Утилита позволяет администратору закрыть туннельное соединение. Если туннельное соединение закрыто, текущее соединение с удаленным рабочим столом прекращается.

После подключения к клиентскому устройству рабочий стол клиентского устройства доступен в окне удаленного подключения Microsoft Windows.

Подключение к существующему сеансу удаленного рабочего стола пользователя осуществляется без уведомления пользователя. Как только вы подключаетесь к сеансу, пользователь устройства автоматически отключается от сеанса без получения уведомления.

Система Virtual Network Computing (VNC)

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- На управляемом устройстве с операционной системой Linux установлен Агент администрирования версии 15.3 или выше.
- На управляемом устройстве с операционной системой Linux установлен VNC-сервер.
- У администратора есть право **Создание туннелирования** для установки туннельного соединения для VNC.
- Порт для туннелирования RDP-соединений открыт (в окне свойств Сервера администрирования в разделе **Порты подключения** включен параметр **Открыть порт для туннельного RDP-подключения**).

Чтобы подключиться к управляемому устройству с операционной системой Linux по VNC с помощью приложения Kaspersky Security Center Web Console, которое открыто на устройстве с операционной системой Windows:

1. В главном меню перейдите в раздел **Управление активами** → **Управляемые устройства** или откройте выборку устройств.
2. Установите флажок рядом с управляемым устройством, к которому вы хотите подключиться удаленно и нажмите на кнопку **Подключиться к удаленному рабочему столу**.

   Откроется окно **Подключиться к удаленному рабочему столу**.

   Если вы выберете несколько устройств, мобильное устройство или устройство с операционной системой macOS, кнопка **Подключиться к удаленному рабочему столу** будет неактивна.
3. В окне **Подключиться к удаленному рабочему столу** выберите тип подключения **VNC**.
4. Скачайте утилиту klsctunnel, нажав на кнопку **Скачать**, и запустите ее.

   Если файл утилиты недоступен для скачивания, отображается сообщение об ошибке. В этом случае скачайте утилиту вручную.
5. В окне **Подключиться к удаленному рабочему столу** укажите порт VNC-подключения. По умолчанию номер порта – 5900.
6. Создайте текстовый BLOB-объект с зашифрованными параметрами подключения, нажав на кнопку **Сгенерируйте BLOB-объект**, скопируйте и вставьте текст в соответствующее поле в утилите klsctunnel.

   BLOB-объект содержит параметры, необходимые для установки соединения между Сервером администрирования и управляемым устройством. BLOB-объект действителен в течение трех минут. Если срок его действия истек, сгенерируйте BLOB-объект повторно.
7. Если вы используете прокси-сервер, в утилите klsctunnel укажите параметры подключения к прокси-серверу.

   Для этого установите флажок **Использовать прокси-сервер** и укажите параметры подключения.
8. Нажмите на кнопку **Открыть порт**.

   Утилита klsctunnel отображает адрес и порт для локального подключения VNC-клиента.

   Утилита позволяет удаленному пользователю закрыть туннельное соединение. Если туннельное соединение закрыто, текущее соединение с удаленным рабочим столом прекращается.
9. Запустите VNC-клиент и подключите его к управляемому устройству, используя адрес и порт, предоставленные утилитой klsctunnel.

Соединение с управляемым устройством установлено. Рабочий стол доступен в окне VNC-клиента.

Удаленный доступ с Windows-устройства с Kaspersky Security Center Web Console к управляемому Windows-устройству

Удаленное подключение к рабочему столу (Remote desktop connection, RDP).

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- На управляемом устройстве с операционной системой Windows установлен Агент администрирования версии 13 или выше.
- У администратора есть право **Запуск RDP-сеансов** для установления RDP-соединений.
- Порт для туннелирования RDP-соединений открыт (в окне свойств Сервера администрирования в разделе **Порты подключения** включен параметр **Открыть порт для туннельного RDP-подключения**).
- Удаленное подключение разрешено в параметрах операционной системы управляемого устройства.

Чтобы подключиться к управляемому устройству с операционной системой Windows по RDP с помощью приложения Kaspersky Security Center Web Console, которое открыто на устройстве с операционной системой Windows:

1. В главном меню перейдите в раздел **Управление активами** → **Управляемые устройства** или откройте выборку устройств.
2. Установите флажок рядом с управляемым устройством, к которому вы хотите подключиться удаленно и нажмите на кнопку **Подключиться к удаленному рабочему столу**.

   Откроется окно **Подключиться к удаленному рабочему столу**.

   Если вы выберете несколько устройств, мобильное устройство или устройство с операционной системой macOS, кнопка **Подключиться к удаленному рабочему столу** будет неактивна.
3. В окне **Подключиться к удаленному рабочему столу** выберите тип подключения **Подключение к удаленному рабочему столу**.
4. Если удаленное подключение не разрешено в параметрах операционной системы управляемого устройства, разрешите удаленное подключение централизованно, нажав на кнопку **Изменить параметры**.

   Если параметры применены правильно, отображается уведомление. Также на управляемом устройстве в разделе **Параметры** → **Система** → **Удаленный рабочий стол** должен быть включен параметр **Включить удаленный рабочий стол**.

   Если удаленное подключение разрешено в параметрах операционной системы управляемого устройства, кнопка **Изменить параметры** не отображается.
5. Скачайте утилиту klsctunnel, нажав на кнопку **Скачать**, и запустите ее.

При скачивании утилиты учитывайте следующее:

- Чтобы получить актуальную версию утилиты klsctunnel убедитесь, что Сервер администрирования имеет доступ к серверам обновлений "Лаборатории Касперского".

  Вы можете запустить задачу *Загрузка обновлений в хранилище Сервера администрирования* и выбрать серверы обновлений "Лаборатории Касперского" в качестве источника обновлений. Если задача завершается успешно, Сервер администрирования имеет доступ к серверам обновлений "Лаборатории Касперского".

- Если файл утилиты недоступен для скачивания, отображается сообщение об ошибке. В этом случае скачайте утилиту вручную и поместите ее на устройство, на котором установлен Сервер администрирования, в директорию /var/opt/kaspersky/klnagent_srv.

6. Создайте текстовый BLOB-объект с зашифрованными параметрами подключения, нажав на кнопку **Сгенерируйте BLOB-объект**, скопируйте и вставьте текст в соответствующее поле в утилите klsctunnel.

   BLOB-объект содержит параметры, необходимые для установки соединения между Сервером администрирования и управляемым устройством. BLOB-объект действителен в течение трех минут. Если срок его действия истек, сгенерируйте BLOB-объект повторно.

7. Если вы используете прокси-сервер, в утилите klsctunnel укажите параметры подключения к прокси-серверу.

   Для этого установите флажок **Использовать прокси-сервер** и укажите параметры подключения.

8. Нажмите на кнопку **Открыть порт**.

   Откроется окно входа в систему подключения к удаленному рабочему столу.

9. Укажите учетные данные учетной записи, под которой вы в настоящий момент входите в Kaspersky Security Center Web Console, и подключитесь к управляемому устройству.

   Утилита klsctunnel отображает адрес и порт для локального подключения удаленного устройства.

   Утилита позволяет администратору закрыть туннельное соединение. Если туннельное соединение закрыто, текущее соединение с удаленным рабочим столом прекращается.

После подключения к клиентскому устройству рабочий стол клиентского устройства доступен в окне удаленного подключения Microsoft Windows.

Подключение к существующему сеансу удаленного рабочего стола пользователя осуществляется без уведомления пользователя. Как только вы подключаетесь к сеансу, пользователь устройства автоматически отключается от сеанса без получения уведомления.

Совместный доступ к рабочему столу (Windows Desktop Sharing, WDS)

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- На управляемом устройстве с операционной системой Windows установлен Агент администрирования версии 13 или выше.
- У администратора есть право **Подключение к существующим RDP-сеансам** для установки WDS-соединения.

- Лицензия на Системное администрирование доступна.
- На рабочем месте администратора установлена операционная система Microsoft Windows Vista или более поздняя версия. Тип операционной системы устройства, на котором установлен Сервер администрирования, не является ограничением для подключения с помощью совместного доступа к рабочему столу Windows.

  Проверьте, включена ли функция совместного доступа к рабочему столу Windows в вашей версии Windows, и убедитесь, что ключ CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} есть в реестре Windows.
- На клиентском устройстве установлена операционная система Microsoft Windows Vista или более поздняя версия.

Чтобы подключиться к управляемому устройству с операционной системой Windows по VNC с помощью приложения Kaspersky Security Center Web Console, которое открыто на устройстве с операционной системой Windows:

1. В главном меню перейдите в раздел **Управление активами** → **Управляемые устройства** или откройте выборку устройств.
2. Установите флажок рядом с управляемым устройством, к которому вы хотите подключиться удаленно и нажмите на кнопку **Подключиться к удаленному рабочему столу**.

   Откроется окно **Подключиться к удаленному рабочему столу**.

   Если вы выберете несколько устройств, мобильное устройство или устройство с операционной системой macOS, кнопка **Подключиться к удаленному рабочему столу** будет неактивна.
3. В окне **Подключиться к удаленному рабочему столу** выберите тип подключения **Совместный доступ к рабочему столу Windows**.

   Если лицензия на Системное администрирование недоступна, отображается сообщение об ошибке.
4. Скачайте утилиту klsctunnel, нажав на кнопку **Скачать**, и запустите ее.

   Если файл утилиты недоступен для скачивания, отображается сообщение об ошибке. В этом случае скачайте утилиту вручную.
5. В списке доступных пользовательских сеансов, активных в выбранной выборке устройств, выберите сеанс, к которому вы хотите подключиться.

   Удаленный пользователь должен разрешить подключение. Если удаленный пользователь отклоняет подключение или если удаленный пользователь не разрешает подключение в течение периода ожидания, отображается сообщение об ошибке.
6. Создайте текстовый BLOB-объект с зашифрованными параметрами подключения, нажав на кнопку **Сгенерируйте BLOB-объект**, скопируйте и вставьте текст в соответствующее поле в утилите klsctunnel.

   BLOB-объект содержит параметры, необходимые для установки соединения между Сервером администрирования и управляемым устройством. BLOB-объект действителен в течение трех минут. Если срок его действия истек, сгенерируйте BLOB-объект повторно.
7. Если вы используете прокси-сервер, в утилите klsctunnel укажите параметры подключения к прокси-серверу.

   Для этого установите флажок **Использовать прокси-сервер** и укажите параметры подключения.
8. Нажмите на кнопку **Открыть порт**.

   Утилита klsctunnel отображает адрес и порт для локального подключения VNC-клиента.

Утилита позволяет удаленному пользователю закрыть туннельное соединение. Если туннельное соединение закрыто, текущее соединение с удаленным рабочим столом прекращается.

Совместный доступ к рабочему столу запускается в новом окне. Если вы хотите взаимодействовать с устройством, нажмите на значок меню () в верхнем левом углу окна и выберите **Интерактивный режим**.

Управление мобильными устройствами

Управление защитой мобильных устройств через Kaspersky Security Center выполняется с помощью компонента Управление мобильными устройствами. Вам нужно добавить лицензионный ключ на каждое мобильное устройство, чтобы активировать приложение защиты. Если вы планируете управлять мобильными устройствами, принадлежащими сотрудникам вашей организации, включите и настройте Управление мобильными устройствами.

Управление мобильными устройствами позволяет управлять Android-устройствами и iOS-устройствами сотрудников. Защита обеспечивается приложением Kaspersky Endpoint Security для Android и системой управления устройствами iOS, установленными на мобильных устройствах. Эти мобильные приложения обеспечивают защиту мобильных устройств от веб-угроз, вирусов и других приложений, которые представляют собой угрозы. Для централизованного управления через Kaspersky Security Center Web Console необходимо установить следующие веб-плагины управления на устройство, на котором установлено приложение Kaspersky Security Center Web Console:

- Плагин Kaspersky Mobile Devices Protection and Management.

  Плагин Kaspersky Mobile Devices Protection and Management позволяет управлять устройствами на базе Android и iOS в Kaspersky Security Center Web Console.

- Плагин параметров Сервер iOS MDM.

  Плагин параметров Сервера iOS MDM позволяет настраивать параметры Сервера iOS MDM, который используется для подключения iOS-устройств к Серверу администрирования и для управления iOS-устройствами.

Информацию о развертывании защиты и управлении мобильными устройствами см. в справке Kaspersky Security для мобильных устройств и в справке Kaspersky Secure Mobility Management.

Использование Firebase Cloud Messaging

Для своевременной доставки команд на Android-устройства Kaspersky Security Center Linux использует механизм push-уведомлений. Push-уведомления обмениваются между Android-устройствами и Сервером администрирования через Firebase Cloud Messaging (далее также FCM). В Kaspersky Security Center Web Console вы можете указать параметры Firebase Cloud Messaging для подключения Android-устройств к сервису.

Для получения параметров Firebase Cloud Messaging вам необходимо иметь учетную запись Google.

Чтобы включить использование FCM:

1. В главном окне Kaspersky Security Center Web Console выберите **Управление активами** → **Мобильные** → **Устройства**.
2. Откройте меню с тремя точками (⋮) и выберите **Синхронизация Android-устройств**.
3. В поле **Номер проекта Firebase** укажите идентификатор отправителя FCM.
4. В поле **Закрытый ключ** выберите файл закрытого ключа.

   При следующей синхронизации с Сервером администрирования Android-устройства будут подключены к службе Firebase Cloud Messaging.

При переключении на другой проект Firebase работа FCM возобновляется через 10 минут.

Сервис FCM работает на следующих диапазонах адресов:

- Со стороны Android-устройства необходим доступ к портам 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS), 5230 (HTTPS) следующих адресов:
  - google.com;
  - fcm.googleapis.com;
  - oauth2.googleapis.com;
  - android.apis.google.com;
  - либо на все IP из списка "Google ASN 15169".
- Со стороны Сервера администрирования необходим доступ на порт 443 (HTTPS) следующих адресов:
  - fcm.googleapis.com;
  - либо на все IP из списка "Google ASN 15169".

Если в свойствах Kaspersky Security Center Web Console заданы параметры прокси-сервера, то для взаимодействия с FCM будут использованы эти параметры.

При изменении значения `strDeviceRegId` устройства в таблице gcm_devices в серверной части FCM синхронизация измененного значения с серверной частью Kaspersky Security Center занимает 5 минут. Во время синхронизации сообщения могут поступать с задержкой на устройство, для которого было изменено значение `strDeviceRegId`.

Настройка FCM: получение Sender ID и файла закрытого ключа

Чтобы настроить FCM:

1. Зарегистрируйтесь на портале Google.
2. Перейдите в консоль Firebase.
3. Выполните одно из следующих действий:
   - Чтобы создать проект, нажмите на кнопку **Create a project** и следуйте инструкциям на экране.
   - Откройте существующий проект.
4. Нажмите на значок шестеренки и выберите **Project settings**.
   Откроется окно **Параметры проекта**.
5. Выберите вкладку **Cloud Messaging**.
6. Скопируйте Sender ID из поля **Sender ID** в разделе **Firebase Cloud Messaging API (V1)**.
7. Выберите вкладку **Service accounts** и нажмите на кнопку **Generate new private key**.
8. В открывшемся окне нажмите на кнопку **Generate key**, чтобы сгенерировать и загрузить файл приватного ключа.

Firebase Cloud Messaging настроен.

Интеграция с инфраструктурой открытых ключей

Вы можете интегрировать выпуск сертификатов с помощью Microsoft Certification Authority (CA) через инфраструктуру открытых ключей (PKI). Интеграция с PKI предназначена для упрощения выдачи сертификатов доменным пользователям Сервером администрирования. В результате интеграции выписка сертификатов происходит автоматически.

Подробную информацию о настройке интеграции с PKI для выпуска сертификатов см. в справке Kaspersky Secure Mobility Management.

Вы можете выполнить интеграцию PKI с указанными параметрами и назначить PKI в качестве источника сертификатов для определенных типов сертификатов. Параметры интеграции PKI позволяют вам установить индивидуальный шаблон по умолчанию для всех типов сертификатов.

Особенности использования интеграции PKI для выпуска сертификатов:

- Интеграция PKI выключена по умолчанию. Подробную информацию о включении PKI и настройке его параметров см. в справке Kaspersky Secure Mobility Management.

- Выдача сертификатов осуществляется с использованием Агента администрирования для Windows. Это обеспечивает интеграцию между Сервером администрирования и Microsoft CA. Поскольку может быть несколько устройств с установленным Агентом администрирования, вы можете указать устройство, которое будет подключаться к Microsoft CA в **Правила выпуска**. Это устройство должно иметь установленный сертификат Enrollment Agent (EA) в хранилище сертификатов учетной записи, под которой выполняется интеграция с PKI. Сертификат выдается администратором CA домена.

- Учетная запись, под которой выполняется интеграция с PKI, должна быть доменным пользователем и иметь право *Вход в качестве службы*.

- Kaspersky Security Center Linux может работать только с одной интеграцией PKI (Microsoft CA) за раз.

Управление группами администрирования

Этот раздел содержит информацию о работе с группами администрирования.

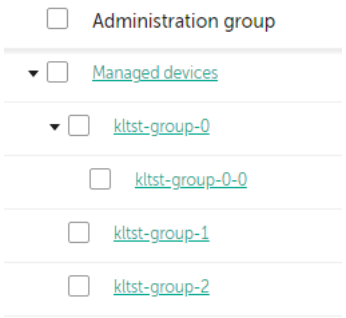
Вы можете выполнять с группами администрирования следующие действия:

- добавлять в состав группы администрирования произвольное количество вложенных групп любых уровней иерархии;
- добавлять в состав групп администрирования устройства;
- изменять иерархию групп администрирования путем перемещения отдельных устройств и целых групп в другие группы;
- удалять из состава групп администрирования вложенные группы и устройства;
- добавлять в состав групп администрирования подчиненные и виртуальные Серверы администрирования;
- переносить устройства из состава групп администрирования одного Сервера в группы администрирования другого Сервера;
- определять, какие приложения "Лаборатории Касперского" будут автоматически устанавливаться на устройства, включаемые в состав группы.

Эти действия можно выполнять, только если у вас есть право **Изменение** в **области** Управление группами администрирования для групп, которыми вы хотите управлять, или для Сервера администрирования, к которому относятся эти группы.

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).

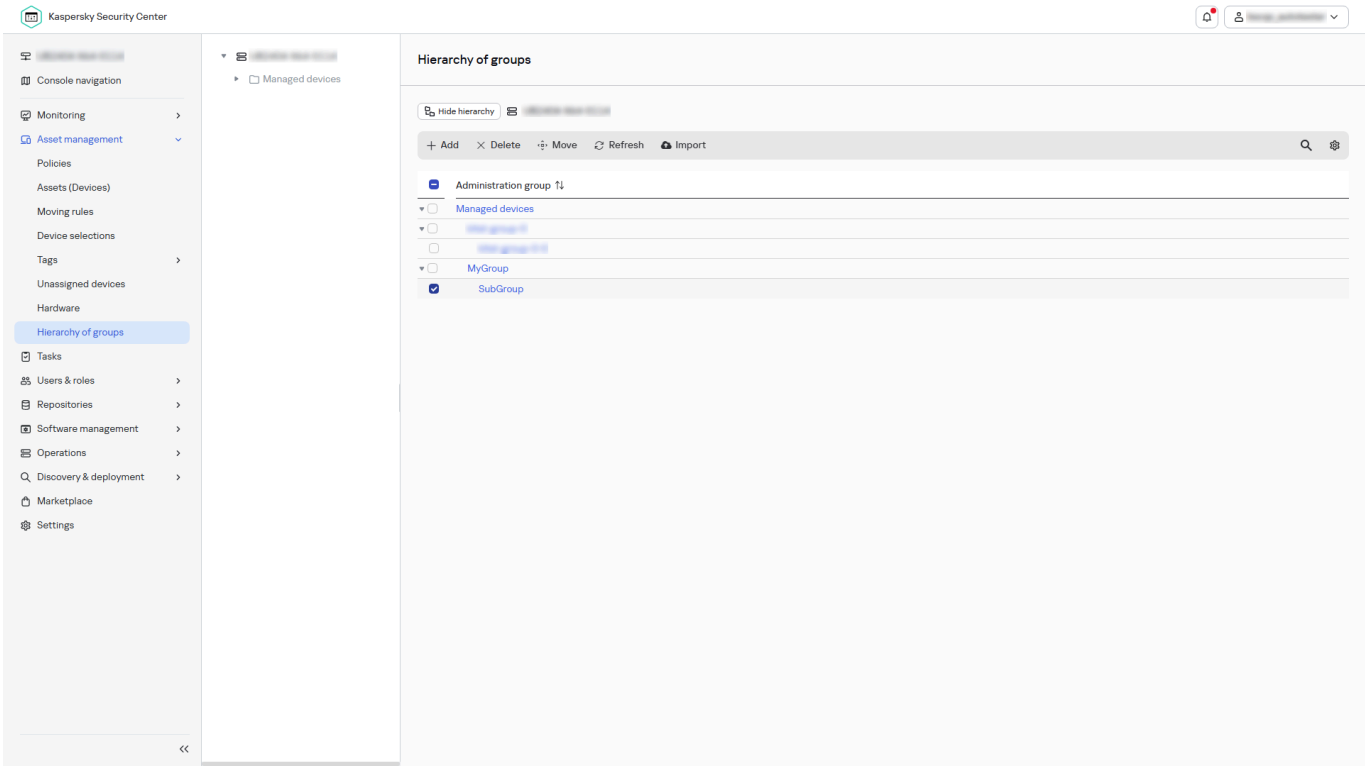


Просмотр иерархии групп администрирования

Чтобы создать группу администрирования:

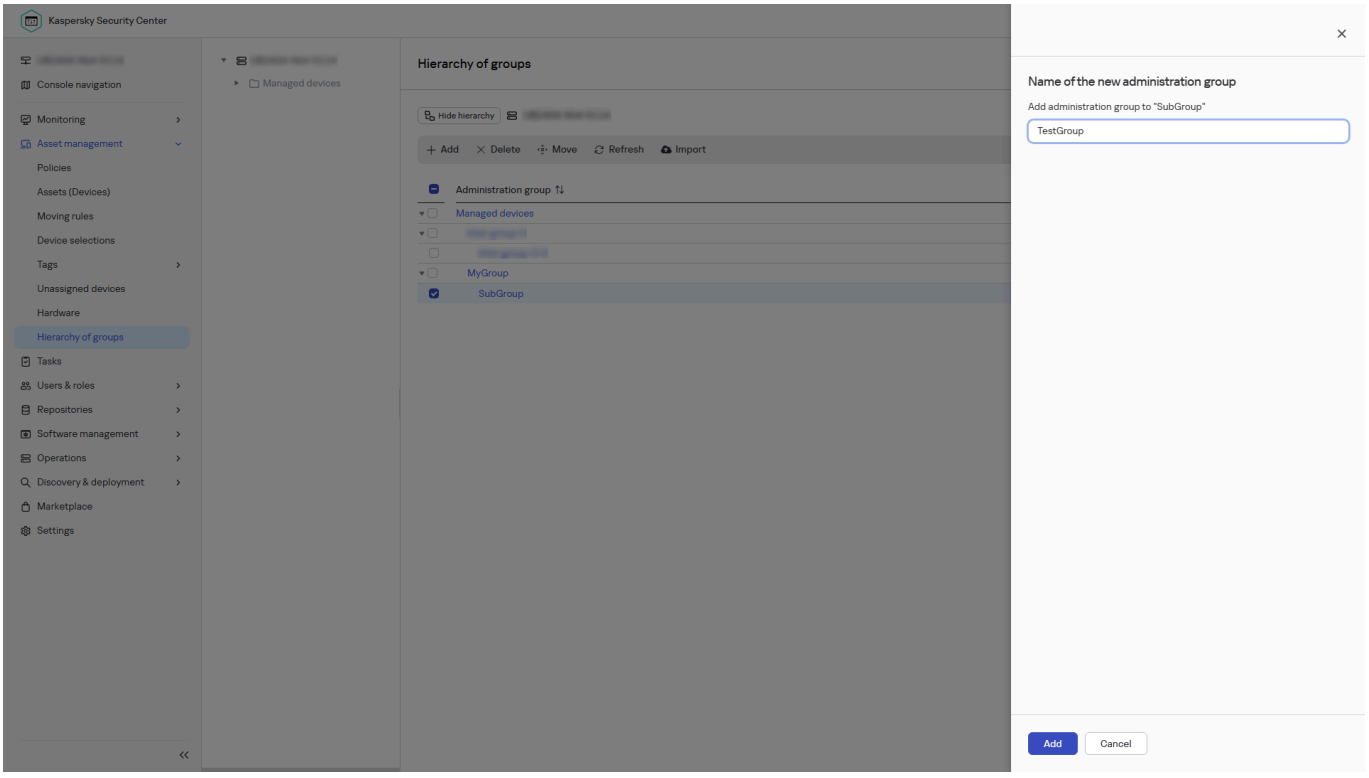
1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп**.

2. В структуре группы администрирования выберите группу администрирования, в состав которой должна входить новая группа администрирования.



3. Нажмите на кнопку **Добавить**.

4. В открывшемся окне **Имя новой группы администрирования** введите имя группы и нажмите на кнопку **Добавить**.



В результате в иерархии групп администрирования появится новая группа администрирования с заданным именем.

Чтобы создать структуру групп администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп**.
2. Нажмите на кнопку **Импортировать**.

В результате запускается мастер создания структуры групп администрирования. Следуйте далее указаниям мастера.

Автоматическая установка приложений на устройства группы администрирования

Вы можете указать, какие инсталляционные пакеты нужно использовать для автоматической удаленной установки приложений "Лаборатории Касперского" на клиентские устройства в группе администрирования.

Чтобы настроить автоматическую установку приложений на устройства в группе администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп**.
2. Перейдите к свойствам нужной группы администрирования одним из следующих способов:
   - Выберите имя группы администрирования.
   - Нажмите на кнопку **Показать иерархию** в верхней части страницы. В открывшейся панели наведите курсор мыши на название нужной группы и нажмите на значок параметров (⚙).

   Откроется окно свойств группы администрирования.
3. В окне свойств перейдите на вкладку **Автоматическая установка**.
4. Выберите инсталляционные пакеты приложений, которые необходимо установить на устройства, и нажмите на кнопку **Сохранить**.

   Если выбрано несколько инсталляционных пакетов одного и того же приложения, отличающихся только версиями, сохраняется инсталляционный пакет с последней версией.

После выбора инсталляционных пакетов, для каждого приложения создается группа задач для установки приложений на устройства в группе администрирования. Эти задачи будут запускаться на клиентских устройствах сразу после их добавления в группу администрирования.

Перемещение групп администрирования

Вы можете перемещать вложенные группы администрирования внутри иерархии групп.

Группа администрирования перемещается вместе со всеми вложенными группами, подчиненными Серверами администрирования, устройствами, групповыми политиками и задачами. К ней будут применены все параметры, соответствующие ее новому положению в иерархии групп администрирования.

Имя группы должно быть уникальным в пределах одного уровня иерархии. Если в папке, в которую вы перемещаете группу администрирования, уже существует группа с аналогичным названием, перед перемещением название группы следует изменить. Если вы предварительно не изменили название перемещаемой группы, к ее названию при перемещении автоматически добавляется окончание вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Вы не можете изменить название группы **Управляемые устройства** или переместить ее.

Чтобы переместить группу администрирования на другой уровень иерархии групп администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп** и установите флажок рядом с группой администрирования, которую вы хотите переместить.
2. Нажмите на кнопку **Переместить** в панели инструментов.
3. В открывшемся окне выберите, куда вы хотите переместить группу администрирования, и нажмите на кнопку **Переместить**.

Окно закрывается и группа администрирования перемещается на другой уровень в иерархии групп.

Удаление групп администрирования

Если вы удалите группу администрирования, содержащую подчиненные Серверы администрирования, вложенные группы, клиентские устройства, групповые задачи или политики, созданные для этой группы, все они также будут удалены.

Перед удалением группы администрирования требуется удалить из ее состава подчиненные Серверы администрирования, вложенные группы и клиентские устройства.

Чтобы удалить группу администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп** и установите флажок рядом с группой администрирования, которую вы хотите удалить.
2. В панели инструментов нажмите на кнопку **Удалить**.

Группа администрирования удалена.

Развертывание приложений "Лаборатории Касперского"

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

Сценарий: развертывание приложений "Лаборатории Касперского"

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

Следующие приложения доступны для развертывания с помощью Kaspersky Security Center Web Console:

- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Windows

Этапы

Развертывание приложений "Лаборатории Касперского" состоит из следующих этапов:

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

   Этот этап обрабатывается мастером первоначальной настройки. Если вы решите не запускать мастер, загрузите плагины вручную.

2. **Загрузка и создание инсталляционных пакетов**

   Этот этап обрабатывается мастером первоначальной настройки.

   Мастер первоначальной настройки позволяет загрузить инсталляционный пакет совместно с веб-плагином управления. Если вы не выбрали этот параметр при запуске мастера или не запускали мастер, требуется загрузить инсталляционный пакет вручную.

   Если вы не можете установить приложения "Лаборатории Касперского" с помощью Kaspersky Security Center Linux на некоторых устройствах, например, на устройствах удаленных сотрудников, вы можете создавать автономные установочные пакеты для приложений. Если вы используете автономные пакеты для установки приложений "Лаборатории Касперского", вам не нужно создавать и запускать задачу удаленной установки, а также создавать и настраивать задачи для Kaspersky Endpoint Security для Windows.

   Также можно загрузить дистрибутивы Агента администрирования и приложений безопасности с сайта "Лаборатории Касперского". Если удаленная установка приложений по каким-либо причинам невозможна, вы можете использовать загруженные дистрибутивы для локальной установки приложений.

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

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

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

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

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

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

4. **Создание и настройка задач**

   Задача *Обновление* Kaspersky Endpoint Security должна быть настроена.

   Этот шаг входит в мастер первоначальной настройки: задача создается и настраивается автоматически, с параметрами по умолчанию. Если вы не запускали мастер первоначальной настройки, вам необходимо создать 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.)

5. **Создание политик**

   Создайте политику Kaspersky Endpoint Security 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.

6. **Проверка результатов**

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

Результаты

Завершение сценария дает следующее:

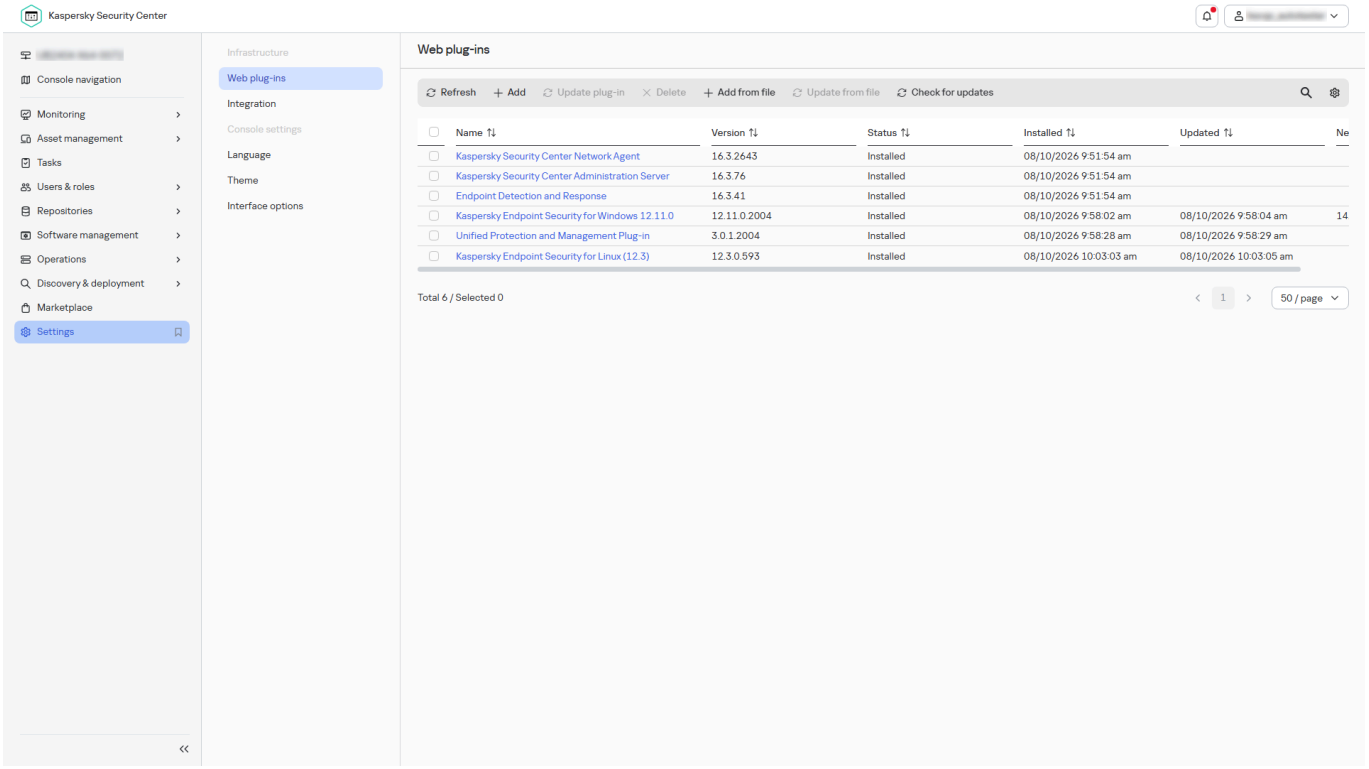
- Все требуемые политики и задачи для выбранных приложений созданы.
- Расписание запуска задач настроено в соответствии с вашими требованиями.
- На выбранных клиентских устройствах развернуты или запланированы к развертыванию выбранные приложения.

Добавление плагина управления для приложений "Лаборатории Касперского"

Чтобы развернуть приложение "Лаборатории Касперского", например Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Windows, необходимо загрузить веб-плагин управления для этого приложения.

Чтобы загрузить веб-плагин управления для приложения "Лаборатории Касперского":

1. В главном меню перейдите в раздел **Параметры** → **Веб-плагины**.



Список установленных веб-плагинов

2. В появившемся окне нажмите на кнопку **Добавить**.

   Отобразится список доступных плагинов управления.

3. В списке доступных плагинов выберите имя плагина, который требуется загрузить (например, Kaspersky Endpoint Security для Linux).

   Отобразится страница с описанием плагина.

4. На странице описания плагина нажмите на кнопку **Установить плагин**.

5. После завершения установки нажмите на кнопку **ОК**.

   Плагин управления будет загружен в конфигурации по умолчанию и появится в списке плагинов управления.

Вы можете добавлять плагины и обновлять загруженные плагины из файла. Вы можете загрузить веб-плагины управления с веб-сайта Службы технической поддержки "Лаборатории Касперского".

Чтобы загрузить или обновить веб-плагин управления из файла:

1. В главном меню перейдите в раздел **Параметры** → **Веб-плагины**.
2. Укажите файл плагина и подпись файла:
   - Нажмите на **Добавить из файла**, чтобы загрузить плагин из файла.
   - Нажмите на **Обновить из файла**, чтобы загрузить обновление для плагина из файла.
3. Укажите файл и подпись файла.
4. Загрузите указанные файлы.

Веб-плагин управления будет загружен из файла и появится в списке веб-плагинов управления.

Инсталляционные пакеты

Инсталляционный пакет – это набор файлов, созданный для удаленной установки приложения "Лаборатории Касперского". Инсталляционный пакет содержит набор параметров, необходимых для установки приложения и обеспечения его работоспособности сразу после установки. Значения параметров соответствуют значениям параметров приложения по умолчанию. Инсталляционный пакет создается на основе файлов с расширениями KPD и KUD, входящих в состав дистрибутива приложения.

Инсталляционные пакеты создаются следующими способами:

- автоматически из указанных дистрибутивов на основании входящих в их состав *описателей* (файлов с расширением kud, содержащих правила установки и анализа результата и другую информацию);
- из архивного файла ZIP, CAB, TAR или TAR.GZ для стандартных или поддерживаемых приложений.

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

Значения параметров установки, специфичные для конкретного поддерживаемого приложения, можно задавать в пользовательском интерфейсе Kaspersky Security Center Web Console при создании инсталляционного пакета. В случае удаленной установки приложений средствами Kaspersky Security Center Linux инсталляционные пакеты доставляются на устройства таким образом, что при запуске инсталлятора приложения ему становятся доступны все заданные администратором параметры. При использовании сторонних средств установки приложений "Лаборатории Касперского" достаточно обеспечить доступность на устройстве всего инсталляционного пакета, то есть дистрибутива и его параметров. Инсталляционные пакеты создаются и хранятся Kaspersky Security Center Linux в соответствующей подпапке папки общего доступа.

Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.

Развертывание с помощью механизма групповых политик Microsoft Windows не поддерживается.

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

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

Загрузка и создание инсталляционных пакетов для приложений "Лаборатории Касперского"

Если у Сервера администрирования есть доступ в интернет, вы можете создавать инсталляционные пакеты для приложений "Лаборатории Касперского" с веб-серверов "Лаборатории Касперского".

Если при создании инсталляционных пакетов для установки приложения на устройства Windows отображается сообщение **Возникла ошибка. Пожалуйста, повторите загрузку**, выполните следующие действия:

1. Создайте флаг RIUtilsArchiveDirUsed с помощью команды:

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Перезапустите службу Сервера администрирования с помощью команды:

   ```
   systemctl restart kladminserver_srv.service
   ```

3. Скачайте дополнительные модули Files for remote installation via Kaspersky Security Center с сайта "Лаборатории Касперского".

   Скачанные архивы имеют следующие имена:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Не переименовывайте архивы.

4. Поместите архивы в директорию /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

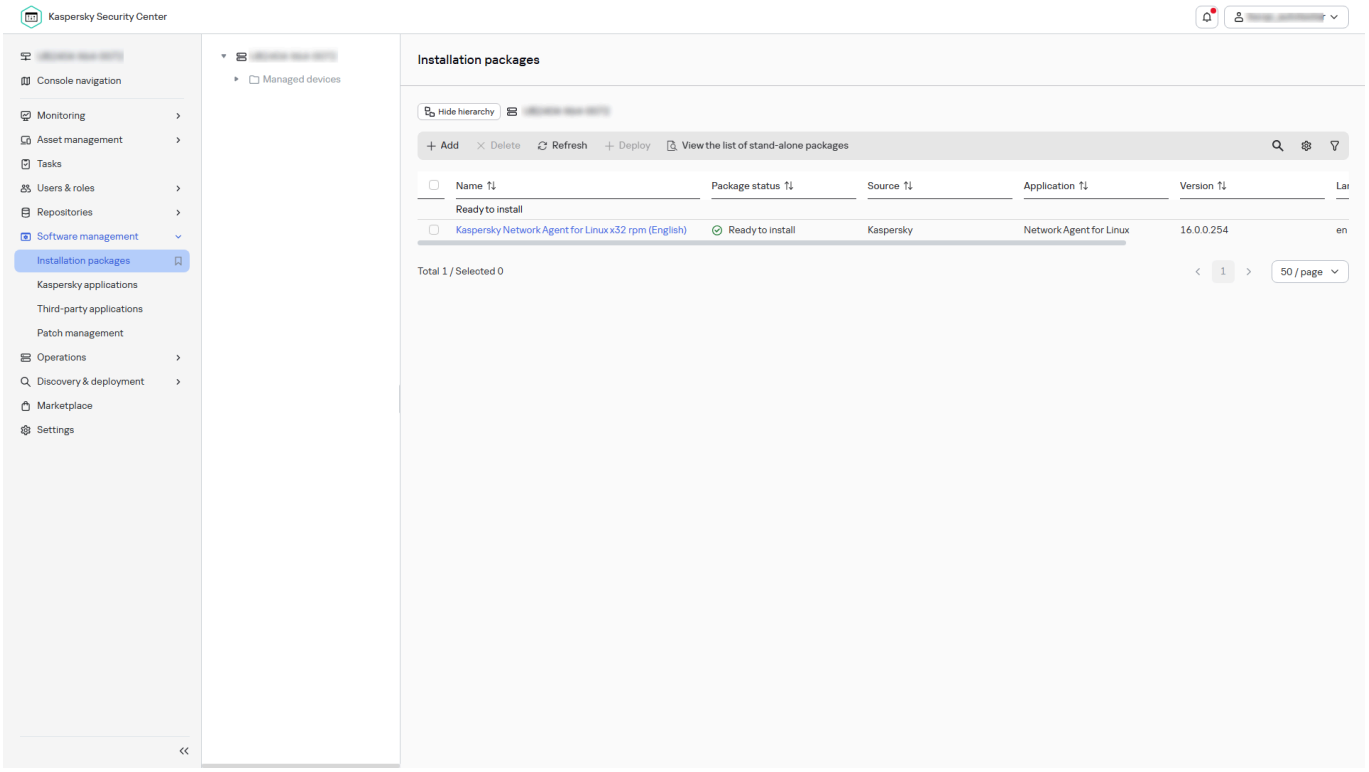
Теперь вы можете создать инсталляционный пакет для установки приложения на устройства Windows.

Чтобы загрузить и создать инсталляционный пакет для приложения "Лаборатории Касперского":

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Инсталляционные пакеты**.

   Вы также можете просматривать информацию о новых пакетах для приложений "Лаборатории Касперского" в списке экранных уведомлений. Если есть уведомления о новом пакете, вы можете перейти по ссылке рядом с уведомлением к списку доступных инсталляционных пакетов.

Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

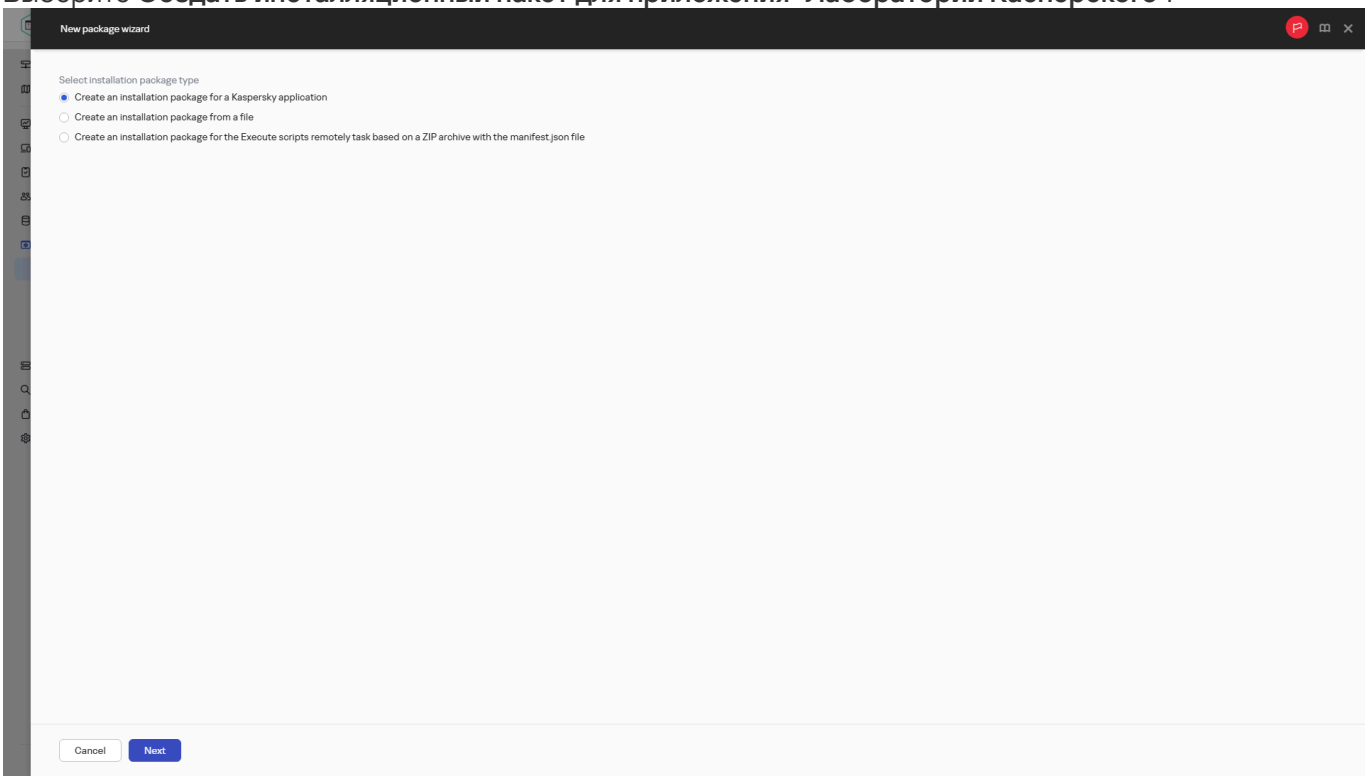


Список инсталляционных пакетов

2. Нажмите на кнопку **Добавить**.

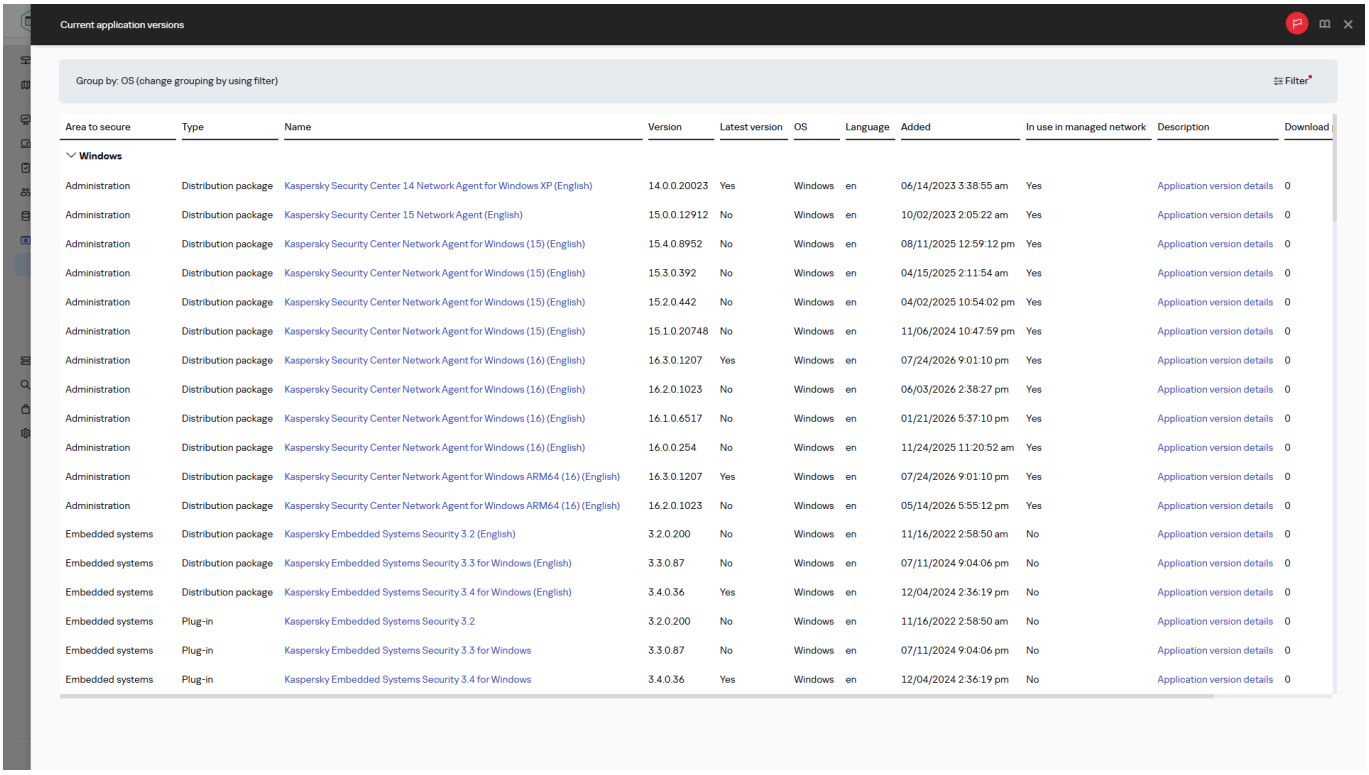
   Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Выберите **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**.



Выбор типа инсталляционного пакета

Отобразится список инсталляционных пакетов доступных на веб-серверах "Лаборатории Касперского". Список содержит инсталляционные пакеты только тех приложений, которые совместимы с текущей версией Kaspersky Security Center Linux. По умолчанию в списке отображаются только приложения на английском языке и на языке, соответствующим языку интерфейса. Чтобы отобразить другие языки, нажмите **Фильтр** и настройте параметры фильтра.



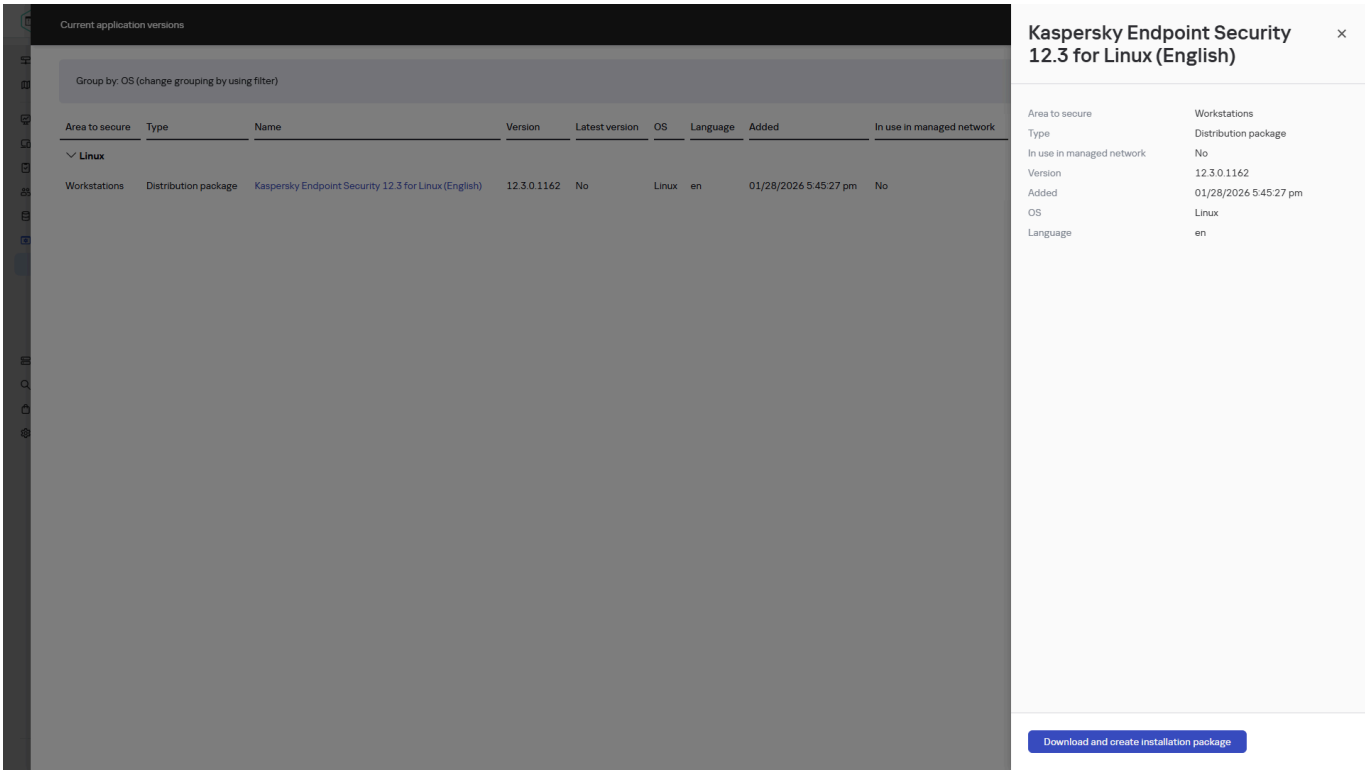
Area to secure	Type	Name	Version	Latest version	OS	Language	Added	In use in managed network	Description	Download
Windows										
Administration	Distribution package	Kaspersky Security Center 14 Network Agent for Windows XP (English)	14.0.0.20023	Yes	Windows	en	06/14/2023 3:38:55 am	Yes	Application version details	0
Administration	Distribution package	Kaspersky Security Center 15 Network Agent (English)	15.0.0.12912	No	Windows	en	10/02/2023 2:05:22 am	Yes	Application version details	0
Administration	Distribution package	Kaspersky Security Center Network Agent for Windows (15) (English)	15.4.0.8952	No	Windows	en	08/11/2025 12:59:12 pm	Yes	Application version details	0
Administration	Distribution package	Kaspersky Security Center Network Agent for Windows (15) (English)	15.3.0.392	No	Windows	en	04/15/2025 2:11:54 am	Yes	Application version details	0
Administration	Distribution package	Kaspersky Security Center Network Agent for Windows (15) (English)	15.2.0.442	No	Windows	en	04/02/2025 10:54:02 pm	Yes	Application version details	0
Administration	Distribution package	Kaspersky Security Center Network Agent for Windows (15) (English)	15.1.0.20748	No	Windows	en	11/06/2024 10:47:59 pm	Yes	Application version details	0
Administration	Distribution package	Kaspersky Security Center Network Agent for Windows (16) (English)	16.3.0.1207	Yes	Windows	en	07/24/2026 9:01:10 pm	Yes	Application version details	0
Administration	Distribution package	Kaspersky Security Center Network Agent for Windows (16) (English)	16.2.0.1023	No	Windows	en	06/03/2026 2:38:27 pm	Yes	Application version details	0
Administration	Distribution package	Kaspersky Security Center Network Agent for Windows (16) (English)	16.1.0.6517	No	Windows	en	01/21/2026 5:37:10 pm	Yes	Application version details	0
Administration	Distribution package	Kaspersky Security Center Network Agent for Windows (16) (English)	16.0.0.254	No	Windows	en	11/24/2025 11:20:52 am	Yes	Application version details	0
Administration	Distribution package	Kaspersky Security Center Network Agent for Windows ARM64 (16) (English)	16.3.0.1207	Yes	Windows	en	07/24/2026 9:01:10 pm	Yes	Application version details	0
Administration	Distribution package	Kaspersky Security Center Network Agent for Windows ARM64 (16) (English)	16.2.0.1023	No	Windows	en	05/14/2026 5:55:12 pm	Yes	Application version details	0
Embedded systems	Distribution package	Kaspersky Embedded Systems Security 3.2 (English)	3.2.0.200	No	Windows	en	11/16/2022 2:58:50 am	No	Application version details	0
Embedded systems	Distribution package	Kaspersky Embedded Systems Security 3.3 for Windows (English)	3.3.0.87	No	Windows	en	07/11/2024 9:04:06 pm	No	Application version details	0
Embedded systems	Distribution package	Kaspersky Embedded Systems Security 3.4 for Windows (English)	3.4.0.36	Yes	Windows	en	12/04/2024 2:36:19 pm	No	Application version details	0
Embedded systems	Plug-in	Kaspersky Embedded Systems Security 3.2	3.2.0.200	No	Windows	en	11/16/2022 2:58:50 am	No	Application version details	0
Embedded systems	Plug-in	Kaspersky Embedded Systems Security 3.3 for Windows	3.3.0.87	No	Windows	en	07/11/2024 9:04:06 pm	No	Application version details	0
Embedded systems	Plug-in	Kaspersky Embedded Systems Security 3.4 for Windows	3.4.0.36	Yes	Windows	en	12/04/2024 2:36:19 pm	No	Application version details	0

Список доступных инсталляционных пакетов

4. Выберите требуемый инсталляционный пакет, например, Kaspersky Endpoint Security для Linux.

   Откроется окно с информацией об инсталляционном пакете.

Вы можете загрузить и использовать инсталляционный пакет, который включает в себя криптографические инструменты, реализующие надежное шифрование, если он соответствует применимым законам и правилам. Чтобы загрузить инсталляционный пакет Kaspersky Endpoint Security для Windows, действительный для нужд вашей организации, обратитесь к законодательству страны, в которой расположены клиентские устройства вашей организации.



Загрузка инсталляционного пакета

5. Ознакомьтесь с информацией и нажмите на кнопку **Скачать и создать инсталляционный пакет**.

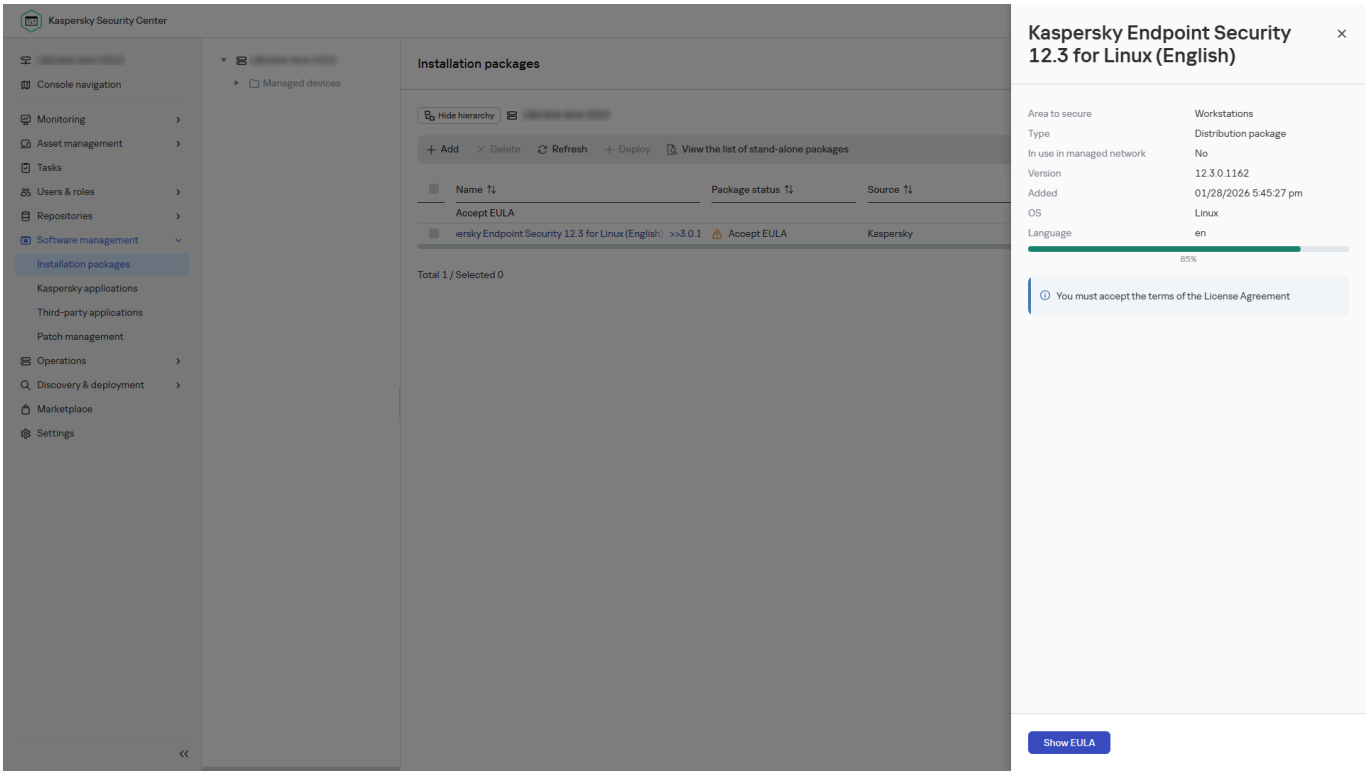
   Если дистрибутив не может быть преобразован в инсталляционный пакет, вместо кнопки **Скачать и создать инсталляционный пакет** отображается кнопка **Скачать дистрибутив**.

Перед процессом загрузки или во время загрузки некоторых приложений "Лаборатории Касперского" отображается кнопка **Показать Лицензионное соглашение**. Если эта кнопка отображается:

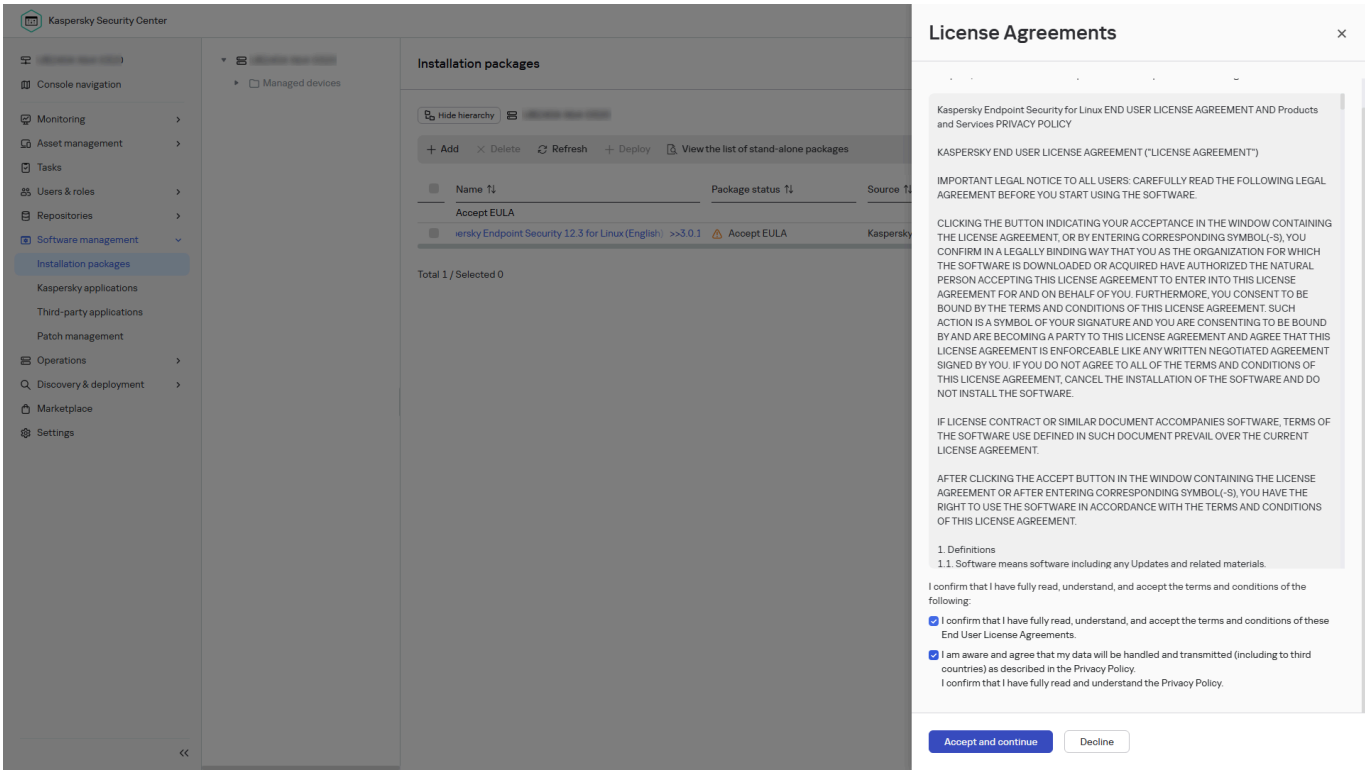
a. Нажмите **Показать Лицензионное соглашение**, чтобы прочитать Лицензионное соглашение.

b. Прочитайте появившееся на экране Лицензионное соглашение и нажмите на кнопку **Принять**.

   Загрузка продолжится после того, как вы примете Лицензионное соглашение. Если вы нажмете на кнопку **Отклонить**, загрузка прекратится.



Загрузка инсталляционного пакета



Принятие Лицензионного соглашения

Вы можете закрыть окно мастера. В этом случае процесс скачивания продолжится в фоновом режиме. Вы можете отслеживать статус загрузки инсталляционного пакета, а также фильтровать и сортировать статусы в столбце **Статус инсталляционного пакета**.

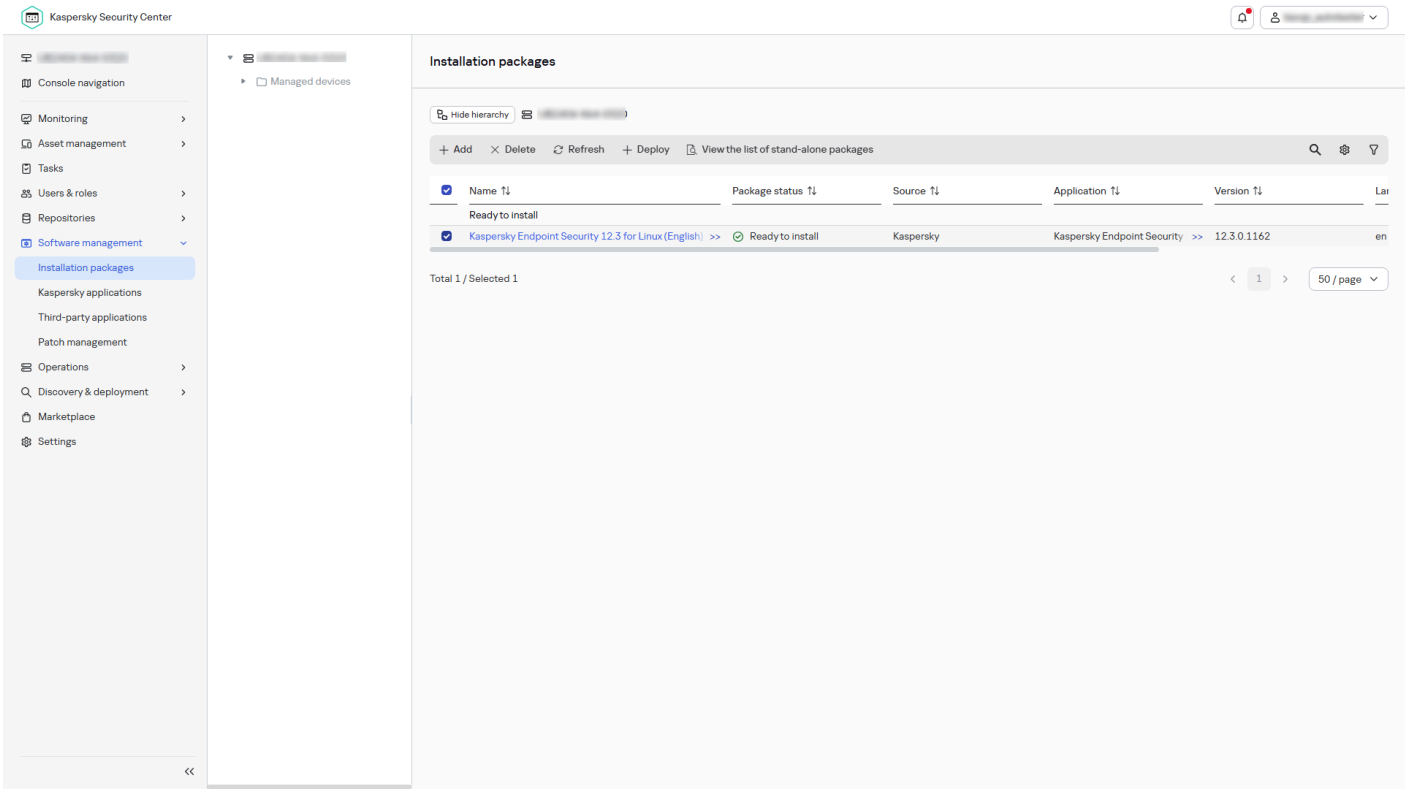
Если процесс загрузки останавливается и статус загрузки меняется на **Принять Лицензионное соглашение**, нажмите на имя инсталляционного пакета и выполните шаги 5.a и 5.b.

Инсталляционные пакеты со статусами **В процессе** и **Принять Лицензионное соглашение** располагаются в начале списка по умолчанию.

Если размер данных, содержащихся в выбранном дистрибутиве, превышает текущее предельное значение, отображается сообщение об ошибке. Вы можете изменить предельное значение и продолжить создание инсталляционного пакета.

6. После завершения загрузки нажмите на кнопку **Закрыть**.

Выбранный инсталляционный пакет загружен в папку общего доступа Сервера администрирования, во вложенную папку Packages. После загрузки инсталляционный пакет отображается в списке инсталляционных пакетов.



Список инсталляционных пакетов

Создание инсталляционных пакетов из файла

Вы можете использовать пользовательские инсталляционные пакеты, чтобы:

- установить любое приложение (такое как текстовый редактор) на клиентские устройства, например, с помощью задачи;
- 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.

Если Сервер администрирования имеет доступ к хранилищу дистрибутивов приложений для удаленной установки, то для загрузки зависимостей, необходимых, чтобы создать инсталляционные пакеты для установки приложений на устройства Windows, используется задача **Загрузка обновлений в хранилище Сервера администрирования**.

Если у Сервера администрирования нет доступа к хранилищу дистрибутивов приложений для удаленной установки, выполните следующие действия:

1. Создайте флаг RlUtilsArchiveDirUsed с помощью команды:

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Скачайте дополнительные модули Files for remote installation via Kaspersky Security Center с сайта "Лаборатории Касперского".

   Скачанные архивы имеют следующие имена:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Не переименовывайте архивы.

3. Поместите архивы в директорию /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

   В противном случае при создании инсталляционного пакета отобразится ошибка **Утилиты удаленной установки win32 не найдены**.

4. Перезапустите службу Сервера администрирования с помощью команды:

   ```
   systemctl restart kladminserver_srv.service
   ```

Теперь у Сервера администрирования есть нужные зависимости.

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

Просмотрите видео, чтобы узнать, как создать и развернуть пользовательский инсталляционный пакет для Windows. Текстовая версия этого руководства для устройств под управлением Windows и Linux доступна ниже.

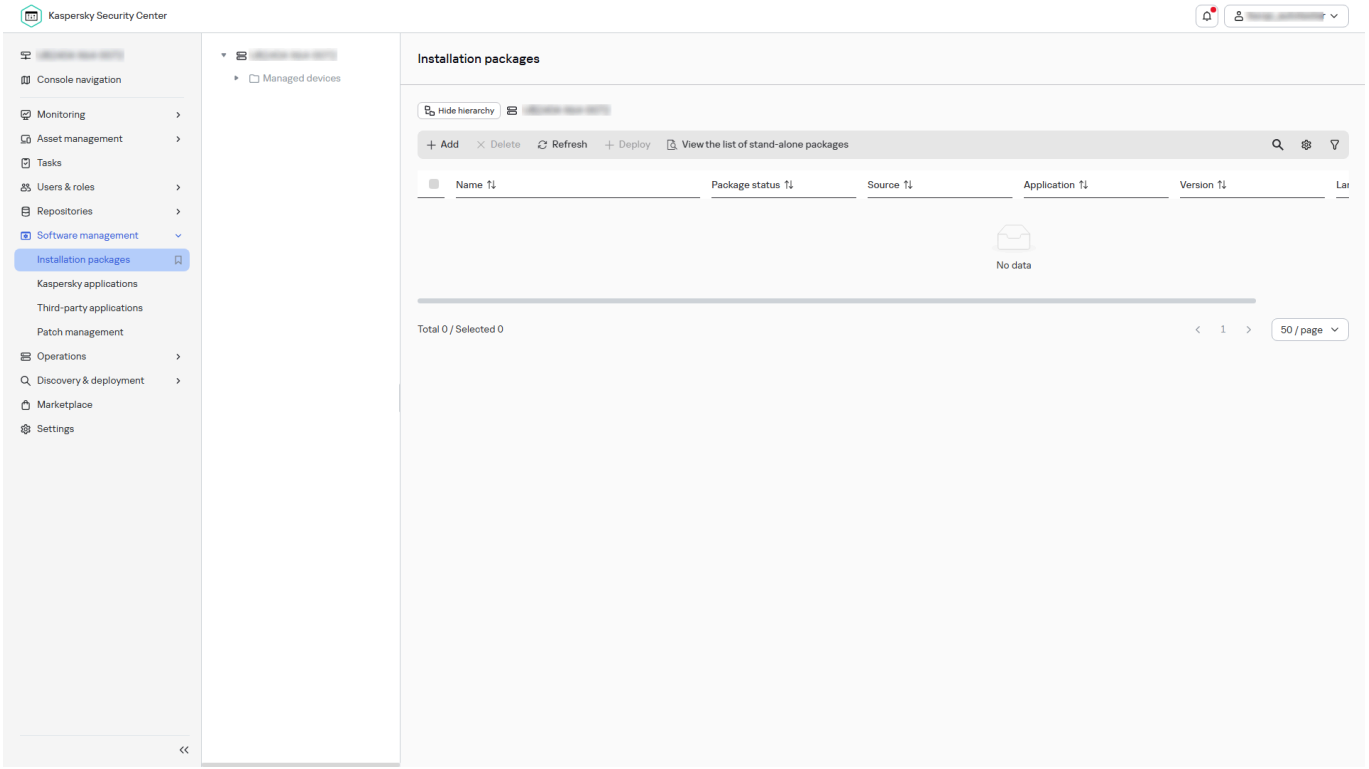


Создание и развертывание пользовательского инсталляционного пакета из файла для Windows. Видео

Чтобы создать пользовательский инсталляционный пакет:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

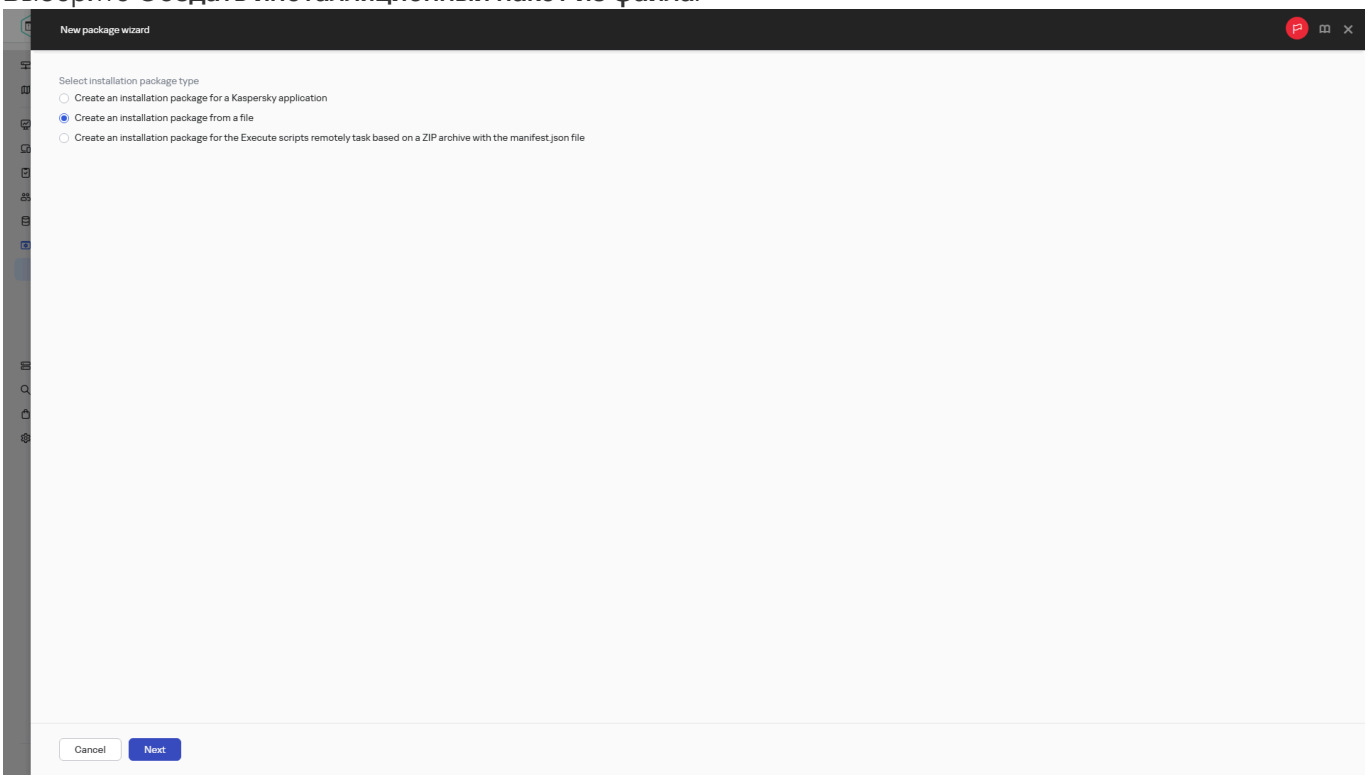


Список инсталляционных пакетов

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**.



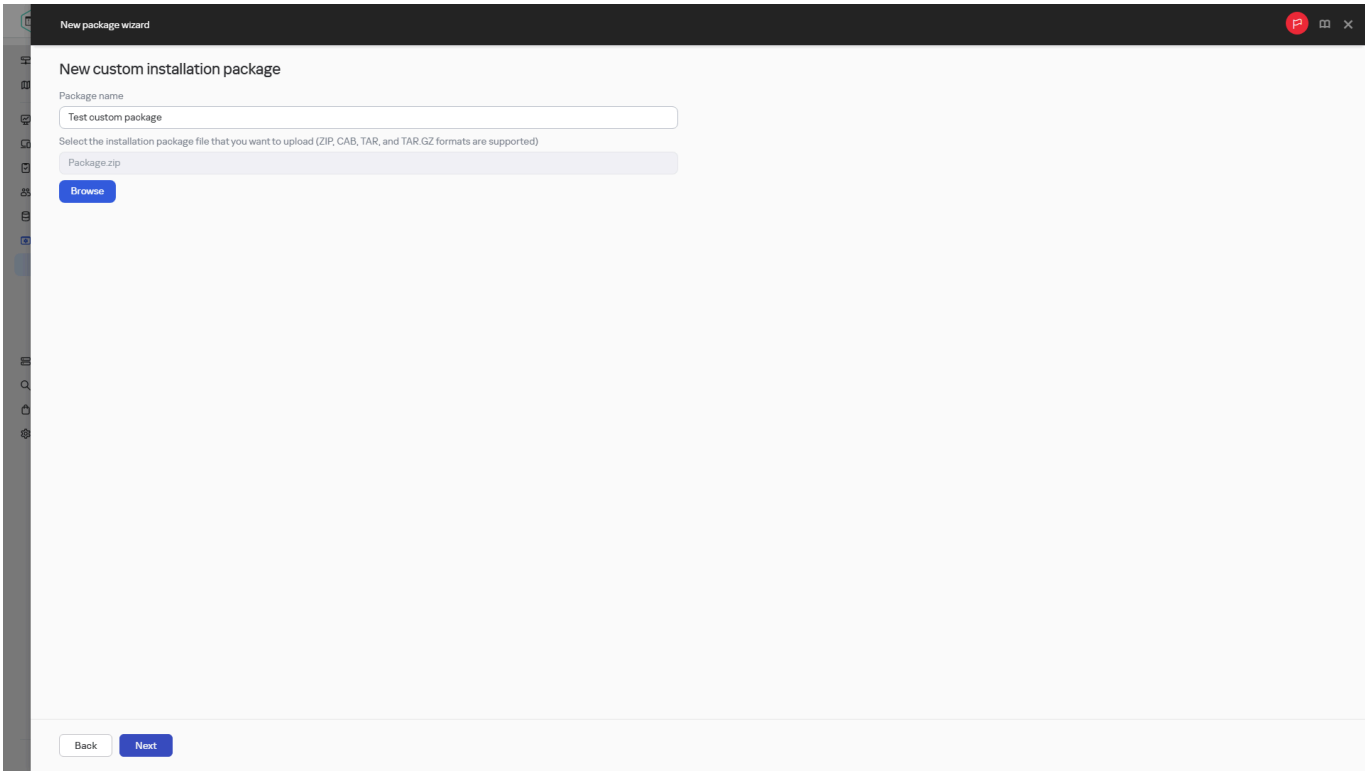
Выбор типа инсталляционного пакета

4. Укажите имя инсталляционного пакета и нажмите на кнопку **Обзор**.

5. В открывшемся окне выберите файл архива, расположенный на доступных дисках.

   Вы можете загрузить архивный файл формата ZIP, CAB, TAR или TAR.GZ. Создать инсталляционный пакет из файла формата SFX (самораспаковывающийся архив) невозможно.

   Начнется загрузка файла на Сервер администрирования.



Указание файла инсталляционного пакета

6. Если вы указали файл приложения "Лаборатории Касперского", вам может быть предложено прочитать и принять Лицензионное соглашение для этого приложения. Чтобы продолжить, вам нужно принять условия Лицензионного соглашения. Выберите параметр **Принять условия и положения 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, вам нужно 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.

   Как создать инсталляционный пакет в формате DEB или RPM

   1. Создайте скрипт `.sh` со следующими командами:

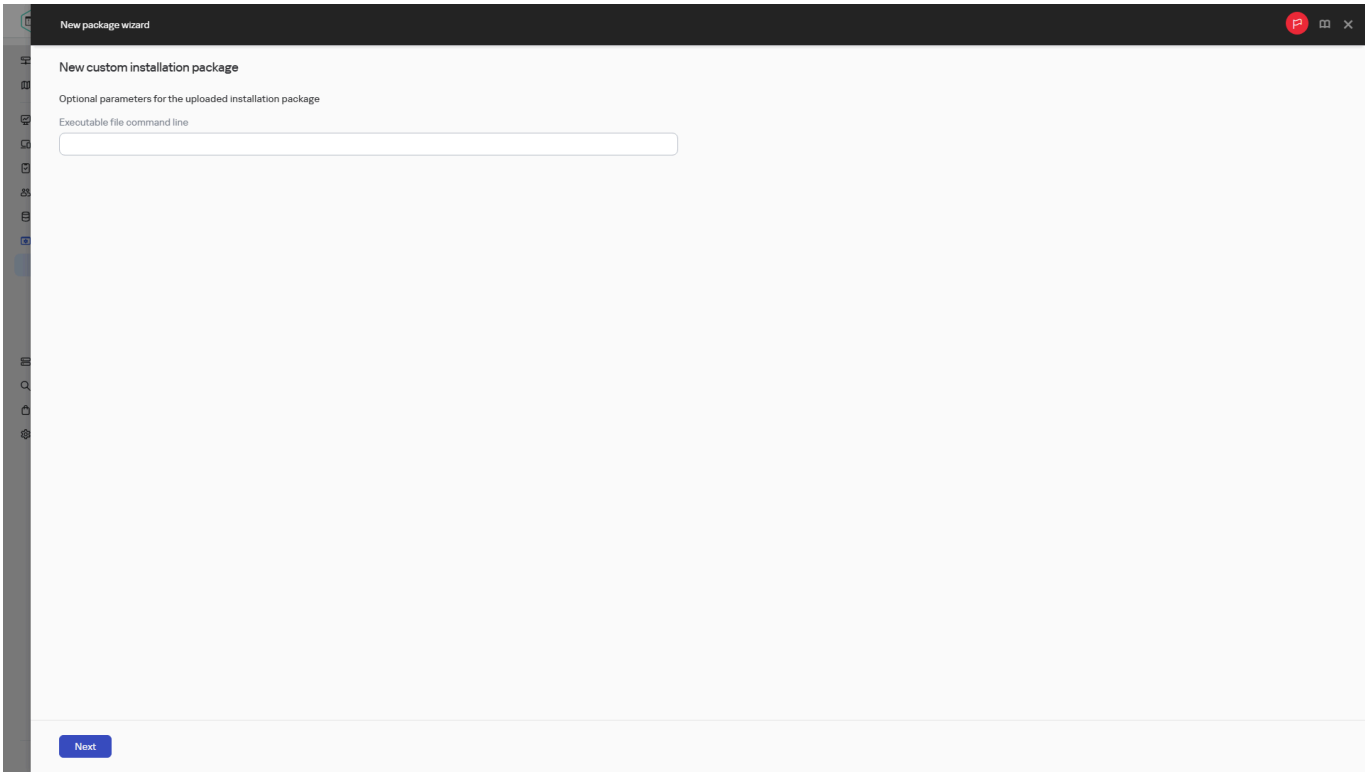
      ```
      #!/bin/sh
      script_dir="$(dirname "$0")"
      apt-get install --yes "$script_dir/<название_пакета>.deb" </dev/null
      ```

      Содержимое скрипта и команды могут различаться в зависимости от формата пакета и других параметров. Вы можете изменить скрипт в соответствии с вашей конфигурацией.

   2. Поместите созданный скрипт в архив вместе с файлом `.deb` или `.rpm`.

   3. При создании инсталляционного пакета выберите созданный скрипт в качестве исполняемого файла.

   Вы можете указать параметры командной строки для установки приложения из инсталляционного пакета в тихом режиме. Указывать параметры командной строки необязательно.



Указание необязательных параметров командной строки

   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.
  - **Статус инсталляционного пакета**. Статус скачивания инсталляционного пакета.
  - **Источник**. Имя поставщика приложения.
  - **Приложение**. Название приложения, упакованного в пользовательский инсталляционные пакет.
  - **Версия**. Версия приложения.
  - **Язык**. Язык приложения, упакованного в пользовательский инсталляционный пакет.
  - **Размер (МБ)**. Размер инсталляционного пакета.
  - **ОС**. 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 приложений на устройства.

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

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

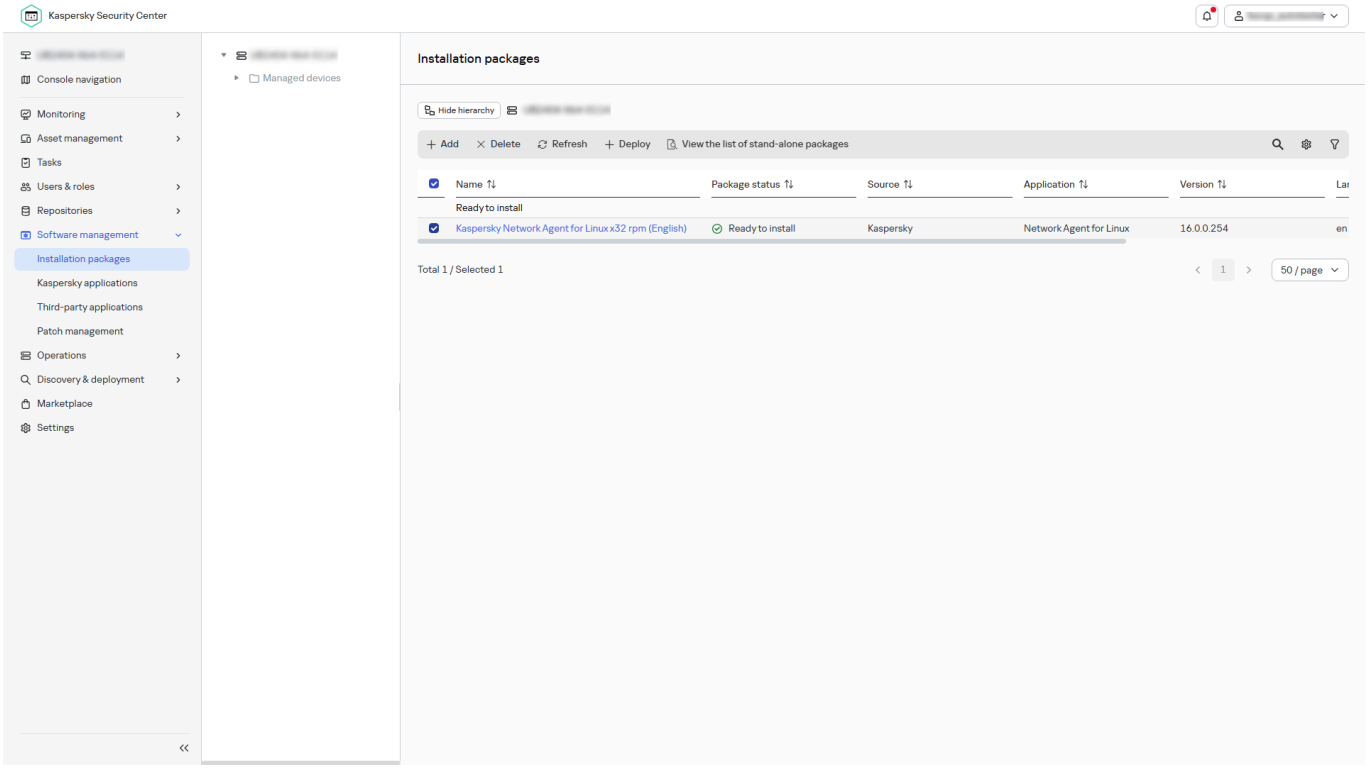
Чтобы создать автономный инсталляционный пакет:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

   > Информация о размере файла, хеше файла и пути отсутствует в списке инсталляционных пакетов для автономного пакета Агента администрирования, а также для пакетов, созданных на виртуальных Серверах администрирования. Эти автономные инсталляционные пакеты генерируются во время загрузки.

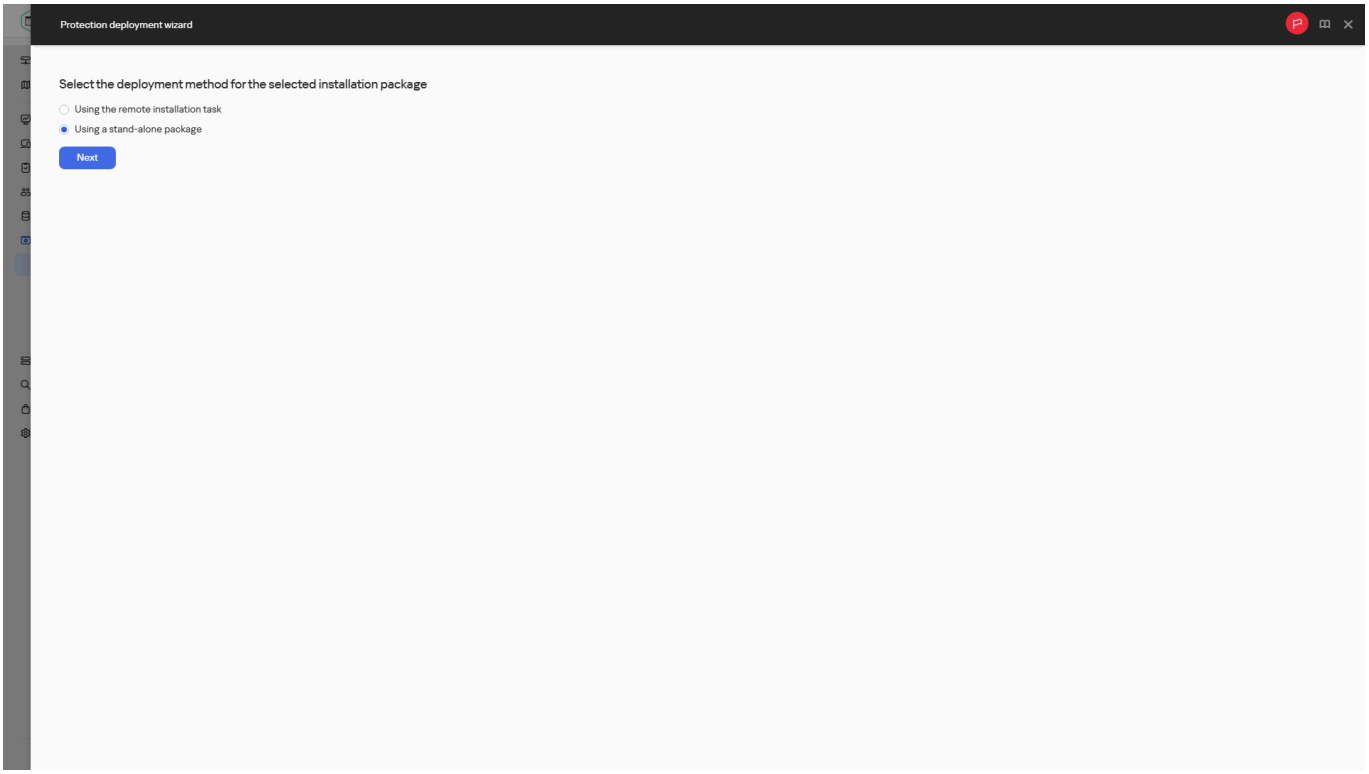
2. В списке инсталляционных пакетов выберите пакет и над списком нажмите на кнопку **Развернуть**.



Список инсталляционных пакетов

3. Выберите параметр **С использованием автономного инсталляционного пакета**.

Запустится мастер создания автономного инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.



Выбор способа развертывания инсталляционного пакета

4. Убедитесь, что включен параметр **Установить Агент администрирования совместно с данным приложением**, если требуется установить Агент администрирования совместно с выбранным приложением.

   Параметр отображается в зависимости от приложения, для которого вы создаете автономный инсталляционный пакет.

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

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

   Если автономный инсталляционный пакет для выбранного приложения уже существует на Сервере администрирования, мастер отобразит сообщение об этом. В этом случае вам нужно выбрать одно из следующих действий:

   - **Создать автономный инсталляционный пакет**. Выберите этот параметр, например, если вы хотите создать автономный инсталляционный пакет для новой версии приложения, и чтобы также остался автономный инсталляционный пакет для предыдущей версии приложения, который вы создали ранее. Новый автономный инсталляционный пакет расположен в другой папке.

   - **Использовать существующий автономный инсталляционный пакет**. Выберите этот параметр, если вы хотите использовать существующий автономный инсталляционный пакет. Процесс создания пакета не запускается.

   - **Сформировать заново существующий автономный инсталляционный пакет**. Выберите этот параметр, если хотите создать автономный инсталляционный пакет для этого же приложения еще раз. Автономный инсталляционный пакет размещается в той же папке.

5. На шаге **Перемещение в список управляемых устройств** параметр **Не перемещать устройства** выбран по умолчанию. Если вы не хотите перемещать клиентское устройство ни в какую группу администрирования после установки Агента администрирования, оставьте этот параметр включенным.

   Если вы хотите переместить клиентское устройство после установки Агента администрирования, выберите параметр **Перемещать нераспределенные устройства в эту группу** и укажите группу администрирования, в которую вы хотите переместить клиентское устройство. По умолчанию устройства перемещаются в группу **Управляемые устройства**.



Выбор группы администрирования для перемещения клиентского 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.

Параметры инсталляционного пакета Агента администрирования

Чтобы настроить параметры инсталляционного пакета Агента администрирования:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. Нажмите на название инсталляционного пакета Агента администрирования.

Откроется окно свойств инсталляционного пакета Агента администрирования.

Параметры инсталляционного пакета Агента администрирования сгруппированы на следующих вкладках:

- Вкладка **Общие**

  На этой вкладке отображается следующая информация об инсталляционном пакете:

  - название инсталляционного пакета;
  - имя и версия приложения, для которого сформирован инсталляционный пакет;
  - размер инсталляционного пакета;
  - дата создания инсталляционного пакета;
  - путь к папке размещения инсталляционного пакета.

- Вкладка **Параметры**

  На этой вкладке можно настроить параметры, необходимые для обеспечения работоспособности Агента администрирования сразу после его установки:

  - Раздел **Параметры**

    Устанавливать в папку по умолчанию

    Если выбран этот вариант, Агент администрирования будет установлен в папку <Диск>:\Program Files\Kaspersky Lab\NetworkAgent. Если такой папки нет, она будет создана автоматически.

    По умолчанию выбран этот вариант.

    Устанавливать в заданную папку

    Если выбран этот вариант, Агент администрирования будет установлен в папку, указанную в поле ввода.

    Использовать пароль деинсталляции

    Если параметр включен, можно ввести пароль для удаления приложения (доступно только для Агента администрирования на устройствах под управлением операционных систем семейства Windows).

    По умолчанию параметр выключен.

    Защитить службу Агента администрирования от неавторизованного удаления, остановки или изменения параметров работы

    Если этот параметр включен, после того, как Агент администрирования был установлен на управляемом устройстве, компонент не может быть удален или изменен без требуемых прав. Работа Агента администрирования не может быть остановлена. Этот параметр не влияет на контроллеры домена.

    Включите этот параметр, чтобы защитить Агент администрирования на рабочих станциях, управляемых с правами локального администратора.

    По умолчанию параметр выключен.

    Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"

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

Если этот параметр выключен, то загруженные обновления и патчи будут установлены только после того, как вы измените их статус на *Одобрено*. Обновления и патчи со статусом *Не определено* не будут установлены.

По умолчанию параметр включен.

- Раздел **Подключение**

  В этом разделе можно настроить параметры подключения Агента администрирования к Серверу администрирования. Для установления соединения можно использовать TLS-протокол или UDP-протокол. Для настройки соединения укажите следующие параметры:

  Адрес Сервера администрирования

  Адрес устройства, на котором установлен Сервер администрирования.

  Номер порта

  Номер порта, по которому будет выполняться подключение.

  SSL-порт

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

  Использовать сертификат Сервера

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

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

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

  По умолчанию параметр выключен.

  Использовать SSL-соединение

  Если этот параметр включен, подключение к Серверу администрирования будет выполняться через защищенный порт с использованием TLS-протокола.

  По умолчанию параметр выключен. Чтобы ваше соединение оставалось безопасным, рекомендуется не выключать этот параметр.

  Использовать UDP-порт

  Если этот параметр включен, подключение Агента администрирования к Серверу администрирования будет выполняться через UDP-порт. Это позволяет управлять клиентскими устройствами и получать информацию о них.

  UDP-порт должен быть открыт на управляемых устройствах, на которых установлен Агент администрирования. Поэтому рекомендуется не выключать этот параметр.

  По умолчанию параметр включен.

  UDP-порт

  В поле можно указать номер порта подключения Сервера администрирования к Агенту администрирования по протоколу UDP.

  По умолчанию номер UDP-порта – 15000.

  Не использовать прокси-сервер

Если этот параметр включен, для подключения устройства к Серверу администрирования используется прямое соединение.

Использовать прокси-сервер

Если этот параметр включен, укажите параметры прокси-сервера:

- **Адрес прокси-сервера**
- **Порт прокси-сервера**

Если ваш прокси-сервер требует аутентификации, включите параметр **Аутентификация на прокси-сервере** и укажите **Имя пользователя** и **Пароль** учетной записи, под которой установлено соединение с прокси-сервером. Рекомендуется указывать данные учетной записи с минимальными правами, необходимыми только для аутентификации на прокси-сервере.

Открывать порты Агента администрирования в брандмауэре Microsoft Windows

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

По умолчанию параметр включен.

> Этот параметр доступен только для инсталляционных пакетов Агента администрирования, предназначенных для устройств с операционной системой Windows.

- Раздел **Дополнительно**

  В этом разделе можно настроить как использовать шлюз соединения.

  В группе параметров **Шлюз соединения** можно настроить способ подключения устройства к Серверу администрирования:

  Использовать в качестве шлюза соединения в демилитаризованной зоне

  Если параметр включен, Агент администрирования выполняет роль шлюза соединения в демилитаризованной зоне (DMZ) для подключения к Серверу администрирования, связи с ним и сохранения данных в безопасности на Агенте администрирования во время передачи данных.

  Подключаться к Серверу администрирования через шлюз соединения

  Если этот параметр включен, подключение к Серверу администрирования с помощью шлюза соединения уменьшает количество подключений к Серверу администрирования. В этом случае введите адрес устройства, которое будет выполнять роль шлюза соединения, в поле **Адрес шлюза соединения**.

  В группе параметров **Виртуальная машина** можно настроить подключение для Virtual Desktop Infrastructure (VDI), если в вашей сети есть виртуальные машины:

  Включить динамический режим для VDI

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

  По умолчанию параметр выключен.

  Оптимизировать параметры для виртуальной машины

  Если параметр включен, в параметрах Агента администрирования выключены следующие функции:

  - получение информации об установленном программном обеспечении;
  - получение информации об аппаратном обеспечении;

- получение информации о наличии уязвимостей;
- получение информации о необходимых обновлениях.

По умолчанию параметр выключен.

Если вы хотите автоматически предлагать пользователям регистрироваться в качестве владельцев устройств после установки Агента администрирования на устройствах под управлением Linux, включите параметр **Разрешить запуск утилиты регистрации пользователя после установки Агента администрирования.**

Если этот параметр включен, после установки Агента администрирования будет запущена утилита регистрации пользователя в качестве владельца устройства. По умолчанию параметр выключен.

- Раздел **Теги**

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

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

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

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

  > Правила автоматического назначения тегов не применяются к инсталляционным пакетам Агента администрирования, предназначенным для устройств под управлением Linux и macOS.

- Вкладка **Автономные пакеты**

  На этой вкладке можно выполнить следующие действия:

  - Просмотреть список автономных инсталляционных пакетов.
  - 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 **Скачать**.
  - Отправить электронное письмо со ссылкой на автономный инсталляционный пакет, нажав на кнопку **Отправить по электронной почте**.
  - Удалить автономный инсталляционный пакет, нажав на кнопку **Удалить**.

- Вкладка **История ревизий**

  На этой вкладке можно просмотреть историю ревизий инсталляционного пакета. Вы можете сравнивать ревизии, просматривать ревизии, сохранять ревизии в файл, добавлять и изменять описания ревизий.

Запуск автономных пакетов, сформированных Kaspersky Security Center Linux

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

При помощи Kaspersky Security Center Linux можно разослать по электронной почте выбранным пользователям ссылку на этот файл в папке общего доступа с просьбой запустить файл (интерактивно или с ключом "тихой" установки "-s"). Автономный инсталляционный пакет можно прикрепить к сообщению электронной почты для пользователей устройств, не имеющих доступа к Веб-серверу. Администратор может скопировать автономный пакет на съемный диск и доставить пакет на нужное устройство с целью его последующего запуска.

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

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

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

Установка приложений с помощью автономных пакетов

Kaspersky Security Center позволяет формировать автономные инсталляционные пакеты приложений. Автономный инсталляционный пакет представляет собой исполняемый файл, который можно разместить на Веб-сервере, отправить по почте или передать на клиентское устройство другим способом. Полученный файл можно запустить локально на клиентском устройстве для выполнения установки приложения без участия Kaspersky Security Center.

Чтобы установить приложение с помощью автономного инсталляционного пакета:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Инсталляционные пакеты**.

2. Установите флажок рядом с инсталляционным пакетом нужного приложения и нажмите на кнопку **Развернуть**.

3. В открывшемся окне выберите **С использованием автономного инсталляционного пакета**, и нажмите на кнопку **Далее**.

   Запустится мастер создания автономного инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. Выберите параметр **Создать автономный инсталляционный пакет**.

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

6. На последнем шаге мастера выберите способ передачи автономного инсталляционного пакета на клиентское устройство и нажмите на кнопку **Готово**, чтобы завершить работу мастера.

7. Передайте автономный инсталляционный пакет приложения на клиентское устройство.

8. Запустите автономный инсталляционный пакет на клиентском устройстве.

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

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

Целесообразность обновления баз в инсталляционном пакете приложения безопасности

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

Изменение ограничения на размер пользовательского инсталляционного пакета

Общий размер данных, распакованных при создании пользовательского инсталляционного пакета, ограничен. Ограничение по умолчанию – 1 ГБ.

Если вы попытаетесь загрузить архивный файл, содержащий данные, превышающие текущее ограничение, появится сообщение об ошибке. Возможно, вам придется увеличить это максимальное значение при создании инсталляционных пакетов из больших дистрибутивов.

Чтобы изменить максимальное значение для размера пользовательского инсталляционного пакета:

1. На устройстве Сервера администрирования запустите командную строку под учетной записью, которая использовалась для установки Сервер администрирования.

2. Измените текущую папку на папку установки Kaspersky Security Center Linux (обычно это /opt/kaspersky/ksc64/sbin).

3. В зависимости от типа установки Сервера администрирования введите одну из следующих команд под учетной записью root:

   - Обычная локальная установка:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <number of bytes>
     ```

   - Установка на отказоустойчивый кластер Kaspersky Security Center Linux:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <number of bytes> --stp klfoc
     ```

   Где <число_байтов> – количество байтов в шестнадцатеричном или десятичном формате.

   Например, если требуемое максимальное значение составляет 2 ГБ, вы можете указать десятичное значение 2147483648 или шестнадцатеричное значение 0x80000000. В этом случае для локальной установки Сервера администрирования вы можете использовать следующую команду:

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

Ограничение на размер пользовательских данных инсталляционного пакета изменено.

Распространение инсталляционных пакетов на подчиненные Серверы администрирования

Kaspersky Security Center Linux позволяет вам создавать инсталляционные пакеты для приложений "Лаборатории Касперского" и для приложений сторонних производителей, а также распространять инсталляционные пакеты на клиентские устройства и устанавливать приложения из пакетов. Для оптимизации нагрузки на главном Сервере администрирования вы можете распространять инсталляционные пакеты на подчиненные Серверы администрирования. После этого подчиненные Серверы передают пакеты на клиентские устройства, после чего вы можете выполнять удаленную установку приложений на свои клиентские устройства.

Чтобы распространить инсталляционные пакеты на подчиненные Серверы администрирования:

1. Убедитесь что подчиненные Серверы администрирования подключены к главному Серверу администрирования.

2. В главном окне приложения перейдите в раздел **Задачи**.

   Отобразится список задач.

3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

4. На странице **Параметры новой задачи** в раскрывающемся списке **Приложение** выберите **Kaspersky Security Center**. Затем в раскрывающемся списке **Тип задачи** выберите **Распространить инсталляционный пакет** и укажите название задачи.

5. На странице **Область действия задачи** выберите устройства, которым назначена задача, одним из следующих способов:

   - Если вы хотите сформировать задачу для всех подчиненных Серверов определенной группы администрирования, выберите эту группу и запустите создание групповой задачи для этой группы.

   - Если вы хотите создать задачу для определенных подчиненных Серверов администрирования, выберите эти Серверы и создайте для них задачу.

6. На странице **Распространяемые инсталляционные пакеты** выберите инсталляционные пакеты, которые необходимо скопировать на подчиненные Серверы администрирования.

7. Укажите учетную запись для запуска задачи *Распространение инсталляционного пакета* под этой учетной записью. Вы можете использовать свою учетную запись и оставить включенным параметр **Учетная запись по умолчанию**. Кроме того, можно указать, что задача должна выполняться под другой учетной записью, имеющей необходимые права доступа. Для этого выберите параметр **Задать учетную запись** и введите учетные данные этой учетной записи.

8. На странице **Завершение создания задачи**, можно включить параметр **Открыть окно свойств задачи после ее создания**, чтобы открыть окно свойств задачи и изменить параметры задачи по умолчанию. Также можно настроить параметры задачи позже в любое время.

9. Нажмите на кнопку **Готово**.

   Задача, созданная для распространения инсталляционных пакетов на подчиненные Серверы администрирования, отображается в списке задач.

10. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

    После выполнения задачи выбранные инсталляционные пакеты скопированы на указанные подчиненные Серверы администрирования.

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 приложения, включенного в пакет.

- **Название приложения**. Имя приложения, которое включено в автономный инсталляционный пакет.

- **Версия приложения**.

- **Имя инсталляционного пакета Агента администрирования**. Параметр отображается только в том случае, если в автономный инсталляционный пакет включен Агент администрирования.

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

Информация о размере файла, хеше файла и пути отсутствует в списке инсталляционных пакетов для автономного пакета Агента администрирования, а также для пакетов, созданных на виртуальных Серверах администрирования. Эти автономные инсталляционные пакеты генерируются во время загрузки.

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 **Скачать**.
- Отправить электронное письмо со ссылкой на автономный инсталляционный пакет, нажав на кнопку **Отправить по электронной почте**.
- Удалить автономный инсталляционный пакет, нажав на кнопку **Удалить**.

Установка Агента администрирования для Linux

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

Предусмотрены следующие способы первоначальной установки Агента администрирования на управляемое устройство с операционной системой Linux:

- Подключиться к управляемому устройству с помощью SSH и запустить задачу удаленной установки.
- Запустить установку инсталляционного пакета на управляемом устройстве.

После установки Агента администрирования на устройство вы можете выполнять удаленную установку приложений "Лаборатории Касперского" на устройстве с помощью этого Агента администрирования. При этом передача дистрибутива устанавливаемого приложения вместе с заданными администратором инсталляционными параметрами осуществляется по каналам связи между Агентами администрирования и Сервером администрирования. Для передачи дистрибутива можно использовать промежуточные центры распространения в виде точек распространения, многоадресную рассылку и прочие средства.

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

- конфигурацию сети организации;
- общее количество устройств;
- наличие в сети организации устройств, не являющихся членами доменов, и наличие унифицированных учетных записей с административными правами на таких устройствах;
- ширину канала между Сервером администрирования и устройствами;
- тип связи между Сервером администрирования и удаленными подсетями и ширину сетевых каналов внутри таких подсетей;
- Параметры безопасности, примененные к удаленным устройствам на момент начала развертывания. Эти параметры позволяют установить удаленное подключение с управляемым устройством и начать установку.

Подготовка устройства с операционной системой Linux к установке Агента администрирования

Перед установкой Агента администрирования на Linux-устройство нужно выполнить подготовительные действия, необходимые для любого Linux-устройства.

Чтобы подготовить устройство с операционной системой Linux к удаленной установке Агента администрирования:

1. Убедитесь, что на устройстве, на которое вы хотите установить Агент администрирования Linux, работает один из поддерживаемых дистрибутивов Linux.

2. Если вы хотите установить Агент администрирования на устройство с операционной системой Альт в режиме замкнутой программной среды, выключите режим замкнутой программной среды до завершения установки.

3. Загрузите инсталляционный пакет Агента администрирования с помощью интерфейса Web Console или с сайта "Лаборатории Касперского".

   Если вам необходимо установить Агент администрирования на устройство под управлением операционной системы Linux с glibc 2.5, вам нужно скачать инсталляционный пакет *Агент администрирования для устаревших версий Linux* с помощью интерфейса Web Console или с сайта "Лаборатории Касперского".

4. 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.
   - Утилита ps.

5. Выполните проверку конфигурации устройства:

   a. Проверьте, что возможно подключение к устройству через SSH (например, приложение PuTTY).

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

      ```
      PasswordAuthentication no
      ChallengeResponseAuthentication yes
      ```

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

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

   b. Убедитесь, что порт TCP 22 открыт и доступен на нераспределенном устройстве с операционной системой Linux.

      Для успешной установки Агента администрирования для Linux должен быть доступен TCP-порт 22.

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

d. Используйте команду `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`

e. Сохраните и закройте файл sudoers.

f. Повторно подключитесь к устройству через SSH и проверьте, что служба sudo не требует пароль, с помощью команды `sudo whoami`.

6. Если вы хотите удаленно установить Агент администрирования на устройствах с операционной системой с системой инициализации systemd, 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`.

Целевое устройство Astra Linux

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.

Целевое устройство ОСнова

Если на целевом устройстве работает ОСнова, выполните следующие действия:

a. Откройте файл `/usr/lib/systemd/logind.conf/10-enable-kill-user-processes.conf` и закомментируйте строку `#KillUserProcess=yes`.

b. Откройте файл `/usr/lib/NESS/pam-user-session` и закомментируйте строку `#loginctl terminate-session "$XDG_SESSION_ID"`.

Чтобы применить измененный параметр, перезапустите устройство под управлением Linux или выполните следующую команду:

```
sudo systemctl restart systemd-logind.service
```

7. 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.

8. 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.

9. Если вы хотите установить Агент администрирования на устройствах под управлением Ubuntu Server или Ubuntu Desktop версии 10.04, выполните дополнительные шаги для подготовки этих устройств.

10. Если вам нужно установить Агент администрирования на устройство под управлением операционной системы Linux с glibc 2.5, выполните дополнительную подготовку целевых устройств.

11. Если вы устанавливаете Агент администрирования на устройство с операционной системой Альт в режиме замкнутой программной среды, повторно включите режим закрытой программной среды.

12. 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.

Linux-устройство готово к установке Агента администрирования. Вы можете установить Агент администрирования удаленно, в интерактивном режиме или в тихом режиме.

Подготовка устройства под управлением SUSE Linux Enterprise Server 15 к установке Агента администрирования

Перед установкой Агента администрирования на устройство под управлением SUSE Linux Enterprise Server 15 вам нужно выполнить две подготовительные процедуры: одну, которая описана в приведенных ниже инструкциях, и общие подготовительные шаги для любого устройства с операционной системой Linux.

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!` Select the `i` option to ignore the warning.

После подготовки Linux-устройства вы можете установить Агент администрирования удаленно, в интерактивном режиме или в тихом режиме.

Подготовка устройства под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования

Перед установкой Агента администрирования на устройство под управлением Astra Linux в режиме замкнутой программной среды вам нужно выполнить две подготовительные процедуры: одну, которая описана в приведенных ниже инструкциях, и общие подготовительные шаги для любого устройства с операционной системой Linux.

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

Чтобы подготовить устройство под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования:

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

   ```
   DIGSIG_ELF_MODE=1
   ```

2. В командной строке введите следующую команду, чтобы установить пакет совместимости:

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

3. Создайте директорию для ключа приложения:

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

4. Поместите ключ приложения /opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg в директорию, созданную на предыдущем шаге:

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

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

5. Обновите оперативную память дисков:

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

   Перезагрузите систему.

Linux-устройство готово к установке Агента администрирования. Вы можете установить Агент администрирования удаленно, в интерактивном режиме или в тихом режиме.

Подготовка к установке Агента администрирования на устройство с операционной системой Linux с glibc 2.5 (устаревшая операционная система)

Перед установкой Агента администрирования на устройство с операционной системой Linux с glibc 2.5 (устаревшая операционная система) вам нужно выполнить две подготовительные процедуры: общие подготовительные шаги для любого устройства с операционной системой Linux и процедуру, приведенную в этой статье.

Рекомендуется использовать локальную установку для установки Агента администрирования на устройство с операционной системой Linux с glibc 2.5 (устаревшая операционная система). Если вам нужно использовать задачу удаленной установки для этого сценария, вам нужно выполнить дополнительные действия, описанные в инструкции ниже.

> Выполните команды, представленные в этой процедуре, под учетной записью root.

Рекомендуется использовать локальную установку для установки Агента администрирования на устройство с операционной системой Linux с glibc 2.5 (устаревшая операционная система). Если вам нужно использовать задачу удаленной установки для этого сценария, вам нужно выполнить дополнительные действия, описанные в инструкции ниже.

1. На устройстве под управлением операционной системы Linux с glibc 2.5 выполните подготовительные шаги, общие для любого устройства с операционной системой Linux.

2. В файле `/etc/sudoers` удалите строку `Defaults requiretty`.

3. Выключите список разрешенных алгоритмов шифрования для SSH-соединений, чтобы иметь возможность установить Агент администрирования на устройстве под управлением Linux с glibc 2.5.

   Для этого на устройстве с установленным Сервером администрирования или на устройстве, выполняющим роль точки распространения, область действия которой включает целевое устройство, в командной строке выполните следующую команду:

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

Linux-устройство готово к удаленной установке Агента администрирования.

Выключение списка разрешенных алгоритмов шифрования может повлиять на безопасность SSH-соединения. Настоятельно рекомендуется повторно включить список разрешенных алгоритмов шифрования сразу после установки Агента администрирования. Чтобы снова включить разрешенный список алгоритмов шифрования, выполните следующую команду:

```
klscflag -fset -pv ".core/.independent" -s "Transport" -n SSH_CLIENT_DISABLE_ALGS_PROTECT
-t d -v 0
```

После установки Агента администрирования и повторного включения разрешенного списка алгоритмов шифрования устройство с операционной системой Linux с glibc 2.5 (устаревшая операционная система), теперь управляется Сервером администрирования.

Подготовка к установке Агента администрирования на устройство с операционной системой OpenSSH версии 6.4 (устаревшая операционная система)

Перед установкой Агента администрирования на устройство, использующее OpenSSH версии 6.4 или ниже (устаревшая операционная система), вам нужно выполнить две подготовительные процедуры: общие шаги подготовки для любого устройства с операционной системой Linux и процедуру, описанную в этой статье.

Рекомендуется использовать локальную установку для установки Агента администрирования на устройство с операционной системой Linux с glibc 2.5 (устаревшая операционная система). Если вам нужно использовать задачу удаленной установки для этого сценария, вам нужно выполнить дополнительные действия, описанные в инструкции ниже.

Выполните команды, представленные в этой инструкции, под учетной записью root.

Чтобы подготовить устройство, использующего OpenSSH версии 6.4 или ниже, для установки Агента администрирования:

1. На устройстве, которое использует OpenSSH версии 6.4 или ниже, выполните подготовительные шаги, общие для любого Linux-устройства.

2. Выключите список разрешенных алгоритмов шифрования для SSH-соединений, чтобы иметь возможность установить Агент администрирования на устройстве под управлением OpenSSH версии 6.4 или ниже.

   Для этого на устройстве с установленным Сервером администрирования или на устройстве, выполняющим роль точки распространения, область действия которой включает целевое устройство, в командной строке выполните следующую команду:

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

Linux-устройство готово к удаленной установке Агента администрирования.

Выключение списка разрешенных алгоритмов шифрования может повлиять на безопасность SSH-соединения. Настоятельно рекомендуется повторно включить список разрешенных алгоритмов шифрования сразу после установки Агента администрирования. Чтобы снова включить разрешенный список алгоритмов шифрования, выполните следующую команду:

```
klscflag -fset -pv ".core/.independent" -s "Transport" -n SSH_CLIENT_DISABLE_ALGS_PROTECT
-t d -v 0
```

После установки Агента администрирования и повторного включения разрешенного списка алгоритмов шифрования устройство с операционной системой Linux с glibc 2.5 (устаревшая операционная система), теперь управляется Сервером администрирования.

Удаленная установка Агента администрирования на устройство с операционной системой Linux

Перед установкой Агента администрирования на устройство с операционной системой Linux нужно выполнить общие подготовительные шаги, которые требуются для всех Linux-устройств.

После выполнения общих шагов вы можете выполнить дополнительные инструкции, в соответствии с вашей операционной системой:

- Подготовка устройства с операционной системой SUSE Linux Enterprise Server 15.
- Подготовка устройства под управлением Astra Linux в режиме замкнутой программной среды.
- Подготовка устройства с операционной системой Ubuntu Server/Desktop версий 10.04 и 16.04.
- Подготовка устройства с операционной системой Linux с glibc 2.5.

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 (приложения, библиотеки) для этого 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. Для создания пакета удаленной установки используйте файлы:

   - klnagent.kpd;
   - akinstall.sh;
   - deb или rpm пакет Агента администрирования.

2. Создайте задачу удаленной установки приложения с параметрами:

   - В окне **Параметры** мастера создания задачи установите флажок **Средствами операционной системы с помощью Сервера администрирования**. Снимите все остальные флажки.
   - На странице **Выбор учетной записи для запуска задачи** укажите параметры учетной записи, которая используется для подключения к устройству через SSH.

3. Запустите задачу удаленной установки приложения. Используйте параметр для команды `su`, чтобы сохранить среду: `-m, -p, --preserve-environment`.

Установка 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.

Перед установкой Агента администрирования на устройство с операционной системой Linux нужно выполнить общие подготовительные шаги, которые требуются для всех Linux-устройств.

После выполнения общих шагов вы можете выполнить дополнительные инструкции, в соответствии с вашей операционной системой:

- Подготовка устройства с операционной системой SUSE Linux Enterprise Server 15.
- Подготовка устройства под управлением Astra Linux в режиме замкнутой программной среды.
- Подготовка устройства с операционной системой Ubuntu Server/Desktop версий 10.04 и 16.04.
- Подготовка устройства с операционной системой Linux с glibc 2.5.

Чтобы выполнить установку Агента администрирования для Linux в тихом режиме:

1. Прочитайте Лицензионное соглашение. Следуйте шагам ниже, только если вы понимаете и принимаете условия Лицензионного соглашения.
2. Создайте файл ответов (в формате TXT). Добавьте в файл ответов список переменных в формате VARIABLE_NAME=variable_value, каждая переменная находится на отдельной строке.

   Для правильного использования файла ответов вам нужно включить в него минимальный набор из трех обязательных переменных:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   Вы также можете добавить любые дополнительные переменные, чтобы использовать более конкретные параметры вашей удаленной установки. В таблице ниже 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 и положения настоящего 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.
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Нет	Позволяет запустить утилиту регистрации пользователя в качестве владельца устройства после установки Агента администрирования. Если выключено, то регистрация в качестве владельца устройства недоступна для пользователя.	1 – после установки Агента администрирования будет запущена утилита регистрации пользователя в качестве владельца устройства. Другое – выключено.
PTCH_ALLOW_APPLY_NONAPROVED_PATCHES	Нет	Определяет, устанавливать ли автоматически загруженные обновления для Агента администрирования со статусом *Не определено*.	true (по умолчанию) – обновления устанавливаются автоматически. false – обновления приложения не устанавливаются автоматически.

3. Запустите инсталляционный пакет Агент администрирования. Переменная среды KLAUTOANSWERS, указывающая путь к файлу ответов, передается в команде для установки. Выполните одну из следующих команд:

   - Чтобы установить Агент администрирования из RPM-пакета на устройство с 32-разрядной операционной системой, выполните команду:
     `sudo KLAUTOANSWERS=<path to the answer file> yum install ./klnagent-<build number>.i386.rpm`

   - Чтобы установить Агент администрирования из RPM-пакета на устройство с 64-разрядной операционной системой, выполните команду:
     `sudo KLAUTOANSWERS=<path to the answer file> yum install ./klnagent64-<build number>.x86_64.rpm`

- Чтобы установить Агент администрирования из RPM-пакета на устройство архитектуры ARM с 64-разрядной операционной системой, выполните команду:
  `sudo KLAUTOANSWERS=<path to the answer file> yum install ./klnagent64-<build number>.aarch64.rpm`

- Чтобы установить Агент администрирования из DEB-пакета на устройство с 32-разрядной операционной системой, выполните команду:
  `sudo KLAUTOANSWERS=<path to the answer file> apt install ./klnagent_<build number>_i386.deb`

- Чтобы установить Агент администрирования из DEB-пакета на устройство с 64-разрядной операционной системой, выполните команду:
  `sudo KLAUTOANSWERS=<path to the answer file> apt install ./klnagent64_<build number>_amd64.deb`

- Чтобы установить Агент администрирования из DEB-пакета на устройство архитектуры ARM с 64-разрядной операционной системой, выполните команду:
  `sudo KLAUTOANSWERS=<path to the answer file> apt install ./klnagent64_<build number>_arm64.deb`

В зависимости от конфигурации операционной системы вы также можете использовать менеджеры пакетов rpm, dpkg или dnf для установки Агента администрирования.

Установка Агента администрирования для Linux начинается в тихом режиме; пользователю не предлагается выполнять никаких действий во время процесса.

Установка Агента администрирования для Linux в интерактивном режиме

В этой статье описывается, как установить Агент администрирования на устройства с операционной системой Linux в интерактивном режиме, указав параметры установки шаг за шагом. Вы также можете использовать файл ответов – текстовый файл, 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.

Перед установкой Агента администрирования на устройство с операционной системой Linux нужно выполнить общие подготовительные шаги, которые требуются для всех Linux-устройств.

После выполнения общих шагов вы можете выполнить дополнительные инструкции, в соответствии с вашей операционной системой:

- Подготовка устройства с операционной системой SUSE Linux Enterprise Server 15.
- Подготовка устройства под управлением Astra Linux в режиме замкнутой программной среды.
- Подготовка устройства с операционной системой Ubuntu Server/Desktop версий 10.04 и 16.04.
- Подготовка устройства с операционной системой Linux с glibc 2.5.

Чтобы установить Агент администрирования в интерактивном режиме:

1. Запустите инсталляционный пакет Агент администрирования. В зависимости от вашего дистрибутива Linux выполните одну из следующих команд:

   - Чтобы установить Агент администрирования из RPM-пакета на устройство с 32-битной операционной системой:

     `# yum -i klnagent-<номер сборки>.i386.rpm`

   - Чтобы установить Агент администрирования из RPM-пакета на устройство с 64-битной операционной системой:

     `# yum -i klnagent64-<номер сборки>.x86_64.rpm`

   - Чтобы установить Агент администрирования из RPM-пакета на устройство с 64-битной операционной системой для Arm-архитектуры:

     `# yum -i klnagent64-<номер сборки>.aarch64.rpm`

   - Чтобы установить Агент администрирования из DEB-пакета на устройство с 32-битной операционной системой:

     `# apt install ./klnagent_<номер сборки>_i386.deb`

   - Чтобы установить Агент администрирования из DEB-пакета на устройство с 64-битной операционной системой:

     `# apt install ./klnagent64_<номер сборки>_amd64.deb`

   - Чтобы установить Агент администрирования из DEB-пакета на устройство с 64-битной операционной системой для Arm-архитектуры:

     `# apt install ./klnagent64_<номер сборки>_arm64.deb`

2. Запустите настройку Агента администрирования:

   `# /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl`

3. Прочитайте Лицензионное соглашение. Текст отображается в окне командной строки. Нажмите пробел, чтобы просмотреть следующий фрагмент текста. При отображении запроса введите одно из следующих значений:

   - Введите `y`, если вы понимаете и принимаете условия Лицензионного соглашения.

   - Введите `n`, если вы не принимаете условия Лицензионного соглашения. Чтобы использовать Агент администрирования, вам нужно принять условия Лицензионного соглашения.

   - Введите `r`, чтобы снова отобразить Лицензионное соглашение.

4. Введите DNS-имя Сервера администрирования или IP-адрес.

5. Введите номер порта Сервера администрирования. По умолчанию номер порта – 14000.

6. Введите номер SSL-порта Сервера администрирования. По умолчанию номер порта – 13000.

7. Введите `y`, если вы хотите использовать SSL-шифрование для трафика между Агентом администрирования и Сервером администрирования. Иначе введите `n`.

8. Выберите один из следующих способов настройки Агента администрирования:

- `[1]` – `Keep current connection gateway settings`.

  В случае первой установки шлюз соединений не будет настроен. В случае обновления будут использоваться ранее заданные параметры шлюза соединений.

- `[2]` – `Do not use connection gateway.`

  Ваше устройство не будет подключаться к Серверу администрирования через шлюз соединения.

- `[3]` – `Connect to server using connection gateway`.

  Ваше устройство будет подключаться к Серверу администрирования через шлюз соединения.

- `[4]` – `Use as connection gateway`.

  Ваше устройство будет выступать в роли шлюза соединения.

Агент администрирования установлен на устройстве с операционной системой Linux.

Поддержка отката файловой системы для устройств с Агентом администрирования

Kaspersky Security Center Linux является распределенным приложением. Откат файловой системы в предыдущее состояние на одном из устройств с установленным Агентом администрирования приведет к рассинхронизации данных и неправильной работе Kaspersky Security Center Linux.

Откат файловой системы (или ее части) в предыдущее состояние может происходить в следующих случаях:

- при копировании образа жесткого диска;
- при восстановлении состояния виртуальной машины средствами виртуальной инфраструктуры;
- при восстановлении данных из резервной копии или точки восстановления.

Для Kaspersky Security Center Linux критичны только те сценарии, при которых стороннее программное обеспечение на устройствах с установленным Агентом администрирования затрагивает директорию /var/opt/kaspersky/klnagent. Поэтому следует всегда исключать эту папку из процедуры восстановления, если это возможно.

Поскольку в ряде организаций регламент работы предполагает выполнение отката состояния файловой системы устройств, в Kaspersky Security Center Linux, начиная с версии 10 Maintenance Release 1 (Сервер администрирования и Агенты администрирования должны быть версии 10 Maintenance Release 1 или выше), была добавлена поддержка обнаружения отката файловой системы на устройствах с установленным Агентом администрирования. В случае обнаружения такие устройства автоматически переподключаются к Серверу администрирования с полной очисткой и полной синхронизацией данных.

В Kaspersky Security Center Linux поддержка обнаружения отката файловой системы включена по умолчанию.

Следует при любой возможности избегать отката директории /var/opt/kaspersky/klnagent на устройствах с установленным Агентом администрирования, так как полная повторная синхронизация данных требует большого количества ресурсов.

Для устройства с установленным Сервером администрирования откат состояния системы недопустим. Недопустимым также является откат в предыдущее состояние базы данных, используемой Сервером администрирования.

Восстановить состояние Сервера администрирования из резервной копии можно только при помощи штатной утилиты klbackup.

Установка Агента администрирования для Windows

Вы можете установить Агент администрирования на устройства с операционной системой Windows в организации для управления ими с помощью Сервера администрирования.

В Microsoft Windows XP Агент администрирования может некорректно выполнять следующие операции: загрузка обновлений напрямую с серверов "Лаборатории Касперского" (если выполняет роль точки распространения); функционирование в качестве прокси-сервера KSN (если выполняет роль точки распространения); обнаружение уязвимостей приложений сторонних производителей (при использовании Системного администрирования).

Перед установкой Агента администрирования на устройство с операционной системой Microsoft Windows на Arm убедитесь, что Агент администрирования для Microsoft Windows x86-64 еще не установлен. Иначе установка не будет выполнена.

Предусмотрены следующие способы первоначальной установки Агента администрирования на управляемое устройство с операционной системой Windows:

- Запустить задачу удаленной установки с помощью точки распространения с операционной системой Windows.

  Перед выполнением удаленной установки на нераспределенном устройстве с операционной системой Windows точка распространения с операционной системой Windows автоматически проверяет UDP-порт 137, чтобы определить тип операционной системы целевого устройства. Если UDP-порт 137 недоступен, точка распространения пытается подключиться к TCP-порту 445 на целевом устройстве, который необходим для выполнения установки.

- С помощью пакета установщика Windows (MSI) для Агента администрирования со сторонними инструментами для удаленной установки приложений.

- Запустить установку приложения на управляемом устройстве.

- Отправить пользователям устройств ссылки на автономные пакеты, сформированные Kaspersky Security Center Linux. Автономные пакеты представляют собой исполняемые модули, содержащие в себе дистрибутивы выбранных приложений с настроенными параметрами.

Установка Агента администрирования для Windows в интерактивном режиме

Чтобы установить Агент администрирования на устройство локально:

1. На устройстве запустите файл ksc_<version number>.<build number>_full_<localization language>.exe из дистрибутива, полученного через интернет.

   Откроется окно с выбором приложений "Лаборатории Касперского" для установки.

2. В окне с выбором приложений по ссылке **Установить только Агент администрирования Kaspersky Security Center** запустите мастер установки Агента администрирования. Следуйте далее указаниям мастера.

   Во время работы мастера установки вы можете настроить дополнительные параметры Агента администрирования (см. ниже).

3. Чтобы использовать устройство в качестве шлюза соединений для выбранной группы администрирования, в окне **Шлюз соединения** мастера установки выберите вариант **Использовать в качестве шлюза соединения в демилитаризованной зоне**.

4. Чтобы настроить Агент администрирования при установке на виртуальную машину:

   a. Если вы планируете создать динамически виртуальные машины из образов виртуальных машин, включите динамический режим Агента администрирования для Virtual Desktop Infrastructure (VDI). Для этого в окне мастера установки **Дополнительные параметры** выберите параметр **Включить динамический режим для VDI**.

      Пропустите этот шаг, если вы не планируете создавать динамически виртуальные машины из образов виртуальных машин.

   b. Оптимизируйте работу Агента администрирования для виртуальной инфраструктуры. Для этого в окне мастера установки **Дополнительные параметры** выберите параметр **Оптимизировать параметры для виртуальной машины**.

      В результате будет выключена проверка исполняемых файлов на наличие уязвимостей при запуске устройства. Также будет выключена передача на Сервер администрирования следующей информации:

      - о реестре оборудования;
      - о приложениях, установленных на устройстве;
      - об обновлениях Microsoft Windows, которые необходимо установить на локальном клиентском устройстве;
      - об уязвимостях в приложениях, обнаруженных на локальном клиентском устройстве.

      В дальнейшем вы сможете включить передачу этой информации в свойствах Агента администрирования или в параметрах политики Агента администрирования.

По окончании работы мастера установки Агент администрирования будет установлен на устройстве.

Вы можете просмотреть свойства службы Агента администрирования, а также запускать, останавливать и контролировать активность Агента администрирования с помощью стандартных инструментов Microsoft Windows: Управление компьютером\Службы.

Установка Агента администрирования для Windows в тихом режиме

Агент администрирования может быть установлен в тихом режиме, то есть без интерактивного ввода параметров установки. Для тихой установки используется инсталляционный пакет (MSI) Агента администрирования. MSI-файл расположен в дистрибутиве приложения Kaspersky Security Center Linux в папке Packages\NetAgent\exec.

Установка Агента администрирования из пакета MSI возможна только в тихом режиме. Интерактивная установка Агента из пакета MSI не поддерживается.

Чтобы установить Агент администрирования на локальном устройстве в тихом режиме:

1. Прочитайте Лицензионное соглашение. Используйте команду ниже, только если вы поняли и принимаете условия Лицензионного соглашения.

2. Выполните команду
   ```
   msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
   ```
   где `setup_parameters` – список параметров и их значений, отделенных друг от друга пробелом (`PROP1=PROP1VAL PROP2=PROP2VAL`).

   В список параметров вам нужно включить параметр `EULA=1`. В противном случае Агент администрирования не будет установлен.

Если вы используете стандартные параметры подключения для Kaspersky Security Center и Агента администрирования на удаленных устройствах, выполните команду:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` – ключ для записи в журнал событий. Журнал событий создается при установке Агента администрирования и сохраняется в папке C:\windows\temp\nag_inst.log.

Помимо nag_inst.log, приложение создает файл $klssinstlib.log, который содержит журнал событий установки. Этот файл хранится в папке %windir%\temp or %temp%. Для устранения неполадок вам или специалисту Службы технической поддержки "Лаборатории Касперского" могут потребоваться оба файла журнала – nag_inst.log и $klssinstlib.log.

Если вам необходимо дополнительно указать порт для подключения к Серверу администрирования, введите команду:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

Параметр `SERVERPORT` соответствует номеру порта подключения к Серверу администрирования.

Имена и возможные значения параметров, которые можно использовать при установке Агента администрирования в тихом режиме, приведены в разделе Параметры установки Агента администрирования.

Если вы хотите обновить Агент администрирования с помощью установщика Windows Installer, выполните следующую команду:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Развертывание захватом и копированием образа устройства

Если нужно инсталлировать Агент администрирования на устройства, на которые также предстоит установить (или переустановить) операционную систему и прочее программное обеспечение, можно воспользоваться механизмом захвата и копирования образа устройства.

Чтобы выполнить развертывание путем захвата и копирования жесткого диска:

1. Создать эталонное устройство с установленной операционной системой и необходимым для работы набором программного обеспечения, включая Агент администрирования и приложение безопасности.

2. Захватить образ "эталонного" устройства и далее распространять этот образ на новые устройства посредством задачи Kaspersky Security Center Linux.

   Для захвата и установки образов дисков используйте сторонние инструменты, доступные в организации.

Копирование образа жесткого диска сторонними инструментами

При использовании сторонних инструментов для захвата образа устройства с установленным Агентом администрирования следует воспользоваться одним из следующих методов:

- На эталонном устройстве остановите службу Агента администрирования и запустите утилиту klmover с ключом `-dupfix`. Утилита klmover входит в состав инсталляционного пакета Агента администрирования. В дальнейшем не допускать запуск службы Агента администрирования вплоть до выполнения операции захвата образа.

- Убедитесь, что перед первым запуском службы Агента администрирования на целевых устройствах утилита klmover запущена с ключом `-dupfix`. Это обязательное требование, которое должно выполняться при первом запуске операционной системы после развертывания образа. Утилита klmover входит в состав инсталляционного пакета Агента администрирования.

- Использовать режим клонирования диска Агента администрирования.

Если образ жесткого диска был скопирован неправильно, вы можете решить эту проблему.

Также можно захватить образ устройства без установленного Агента администрирования. Для этого выполните развертывание образа на целевых устройствах, а затем установите Агент администрирования. При использовании этого метода предоставьте доступ к сетевой папке с автономными инсталляционными пакетами с устройства.

Режим клонирования диска Агента администрирования

Клонирование жесткого диска "эталонного" устройства является распространенным способом установки программного обеспечения на новые устройства. Если Агент администрирования на жестком диске "эталонного" устройства во время клонирования работает в обычном режиме, возникает следующая проблема:

После развертывания на новых устройствах эталонного образа диска с Агентом администрирования эти устройства отображаются в Kaspersky Security Center Web Console как одно устройство. Проблема возникает потому, что при клонировании на новых устройствах сохраняются одинаковые внутренние данные, позволяющие Серверу администрирования связать устройство со своей записью в Kaspersky Security Center Web Console.

Избежать проблемы с неверным отображением новых устройств в Kaspersky Security Center Web Console после клонирования помогает специальный режим *клонирования диска Агента администрирования*. Используйте этот режим, если вы разворачиваете программное обеспечение (с Агентом администрирования) на новых устройствах путем клонирования диска.

В режиме клонирования диска Агент администрирования работает, но не подключается к Серверу администрирования. При выходе из режима клонирования Агент администрирования удаляет внутренние данные, из-за наличия которых Сервер администрирования связывает несколько устройств с одной записью в Kaspersky Security Center Web Console. По завершении клонирования образа эталонного устройства, новые устройства отображаются в Kaspersky Security Center Web Console нормально (как отдельные записи).

Сценарий использования режима клонирования диска Агента администрирования

1. Администратор устанавливает Агент администрирования на "эталонном" устройстве.
2. Администратор проверяет подключение Агента администрирования к Серверу администрирования с помощью утилиты klnagchk.
3. Администратор включает режим клонирования диска Агента администрирования.
4. Администратор устанавливает на устройство программное обеспечение, патчи и выполняет любое количество перезагрузок устройства.
5. Администратор выполняет клонирование жесткого диска "эталонного" устройства на любое число устройств.
6. Для каждой клонированной копии должны быть выполнены следующие условия:
    a. имя устройства изменено;
    b. устройство перезагружено;
    c. режим клонирования диска выключен.

Включение и выключение режима клонирования диска с помощью утилиты klmover

Чтобы включить или выключить режим клонирования диска Агента администрирования:

1. Запустите утилиту klmover на устройстве с установленным Агентом администрирования, который нужно клонировать.

   Утилита klmover находится в папке установки Агента администрирования.

2. Чтобы включить режим клонирования диска, в командной строке Linux введите команду:

   ```
   ./klmover -cloningmode 1
   ```

   Агент администрирования переключается в режим клонирования диска.

3. Чтобы запросить текущее состояние режима клонирования диска, в командной строке введите команду:

   ```
   ./klmover -cloningmode
   ```

   В результате в окне утилиты отобразится информация о том, включен или выключен режим клонирования диска.

4. Чтобы выключить режим клонирования диска, в командной строке утилиты введите команду:

   ```
   ./klmover -cloningmode 0
   ```

Параметры установки Агента администрирования

В таблице ниже описаны свойства MSI, которые можно настраивать при установке Агента администрирования. Все параметры являются необязательными, кроме EULA и SERVERADDRESS.

Параметры установки Агента администрирования в тихом режиме

Свойство MSI	Описание	Доступные значения
EULA	Согласие с условиями Лицензионного соглашения	• 1 – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения настоящего Лицензионного соглашения. • 0 – Я не принимаю условия Лицензионного соглашения (установка не выполняется). • Значение не задано – Я не принимаю условия Лицензионного соглашения (установка не выполняется).
DONT_USE_ANSWER_FILE	Читать параметры установки из файла ответов.	• 1 – Не использовать. • другое значение или не задано – читать.
INSTALLDIR	Путь к папке установки Агента администрирования.	Строковое значение.
SERVERADDRESS	Адрес Сервера администрирования (обязательный параметр).	Строковое значение.
SERVERPORT	Номер порта подключения к Серверу администрирования.	Числовое значение.

Свойство MSI	Описание	Доступные значения
SERVERSSLPORT	Номер порта для защищенного подключения к Серверу администрирования с использованием протокола TLS.	Числовое значение.
USESSL	Использовать ли TLS-соединение.	• 1 – использовать; • другое значение или не задано – не использовать.
OPENUDPPORT	Открыть ли UDP-порт.	• 1 – открывать; • другое значение или не задано – не открывать.
UDPPORT	Номер UDP-порта.	Числовое значение.
USEPROXY	Использовать ли прокси-сервер.	• 1 – использовать; • другое значение или не задано – не использовать.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Адрес прокси-сервера и номер порта для подключения к прокси-серверу.	Строковое значение.
PROXYLOGIN	Учетная запись для подключения к прокси-серверу.	Строковое значение.
PROXYPASSWORD	Пароль учетной записи для подключения к прокси-серверу (Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.)	Строковое значение.
GATEWAYMODE	Режим использования шлюза соединения.	• 0 – не использовать шлюз соединений; • 1 – использовать данный Агент администрирования в качестве шлюза соединений; • 2 – подключаться к Серверу администрирования через шлюз соединений.
GATEWAYADDRESS	Адрес шлюза соединений.	Строковое значение.
CERTSELECTION	Способ получения сертификата.	• GetOnFirstConnection – получить сертификат от Сервера администрирования; • GetExistent – задать существующий сертификат. Если выбран этот вариант, должно быть задано свойство CERTFILE.
CERTFILE	Путь к файлу сертификата.	Строковое значение.
VMVDI	Включить динамический режим для VDI.	• 1 – включать; • 0 – не включать; • Значение не задано – не включать.
LAUNCHPROGRAM	Запускать ли службу Агента администрирования после установки. Параметр игнорируется, если VMVDI=1.	• 1 – запускать; • другое значение или не задано – не запускать.
NAGENTTAGS	Тег для Агента администрирования (имеет приоритет над тегом, указанным в файле ответов).	Строковое значение.

Установка приложений с помощью задачи удаленной установки

Kaspersky Security Center Linux позволяет удаленно устанавливать приложения на устройства с помощью задач удаленной установки. Задачи создаются и назначаются устройствам с помощью мастера. Чтобы быстрее и проще назначить задачу устройствам (до 1000 устройств), вы можете указывать в окне мастера устройства удобным для вас способом:

- **Назначить задачу группе администрирования**. В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.

- **Задать адреса устройств вручную или импортировать из списка**. Вы можете задавать DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

- **Назначить задачу выборке устройств**. В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать выборку, созданную по умолчанию, или вашу собственную выборку. Вы можете выбрать не более 1000 устройств.

Для того чтобы избежать проблем, которые могут возникнуть при установке приложения на клиентское устройство без установленного Агента администрирования, необходимо действовать, как описано в разделе принудительного развертывания с помощью задачи удаленной установки Kaspersky Security Center Linux.

О задачах удаленной установки приложений Kaspersky Security Center Linux

Kaspersky Security Center Linux предоставляет разнообразные механизмы удаленной установки приложений, реализованные в виде задач удаленной установки приложений (принудительная установка, установка с помощью копирования образа жесткого диска). Создать задачу удаленной установки можно как для указанной группы администрирования, так и для набора устройств или для выборки устройств (такие задачи отображаются в Kaspersky Security Center Web Console в папке **Задачи**). При создании задачи можно выбрать инсталляционные пакеты (Агента администрирования и/или другого приложения), подлежащие установке при помощи данной задачи, а также задать ряд параметров, определяющих способ удаленной установки. Кроме того, можно воспользоваться мастером удаленной установки приложений, в основе которого также лежит создание задачи удаленной установки приложений и мониторинг результатов.

Задачи для групп администрирования действуют не только на устройства, принадлежащие этой группе, но и на все устройства всех подгрупп выбранной группы. Если в параметрах задачи включен соответствующий параметр, задача распространяется на устройства подчиненных Серверов администрирования, расположенных в данной группе или ее подгруппах.

Задачи для наборов устройств актуализируют список клиентских устройств при каждом запуске в соответствии с составом выборки устройств на момент запуска задачи. Если в выборке устройств присутствуют устройства, подключенные к подчиненным Серверам администрирования, задача будет запускаться и на этих устройствах. Подробнее об этих параметрах и способах установки будет рассказано далее в этом разделе.

Для успешной работы задачи удаленной установки на устройствах, подключенных к подчиненным Серверам администрирования, следует при помощи задачи ретрансляции предварительно ретранслировать используемые задачей инсталляционные пакеты на соответствующие подчиненные Серверы администрирования.

Удаленная установка приложений

Этот раздел содержит информацию о том, как удаленно установить приложение на устройства в группе администрирования, устройства с определенными адресами или на выборку устройств.

Чтобы установить приложение на выбранные устройства:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В поле **Тип задачи** выберите **Удаленная установка приложения**.
4. Выберите один из следующих вариантов:

   Назначить задачу группе администрирования

   Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

   Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

   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.

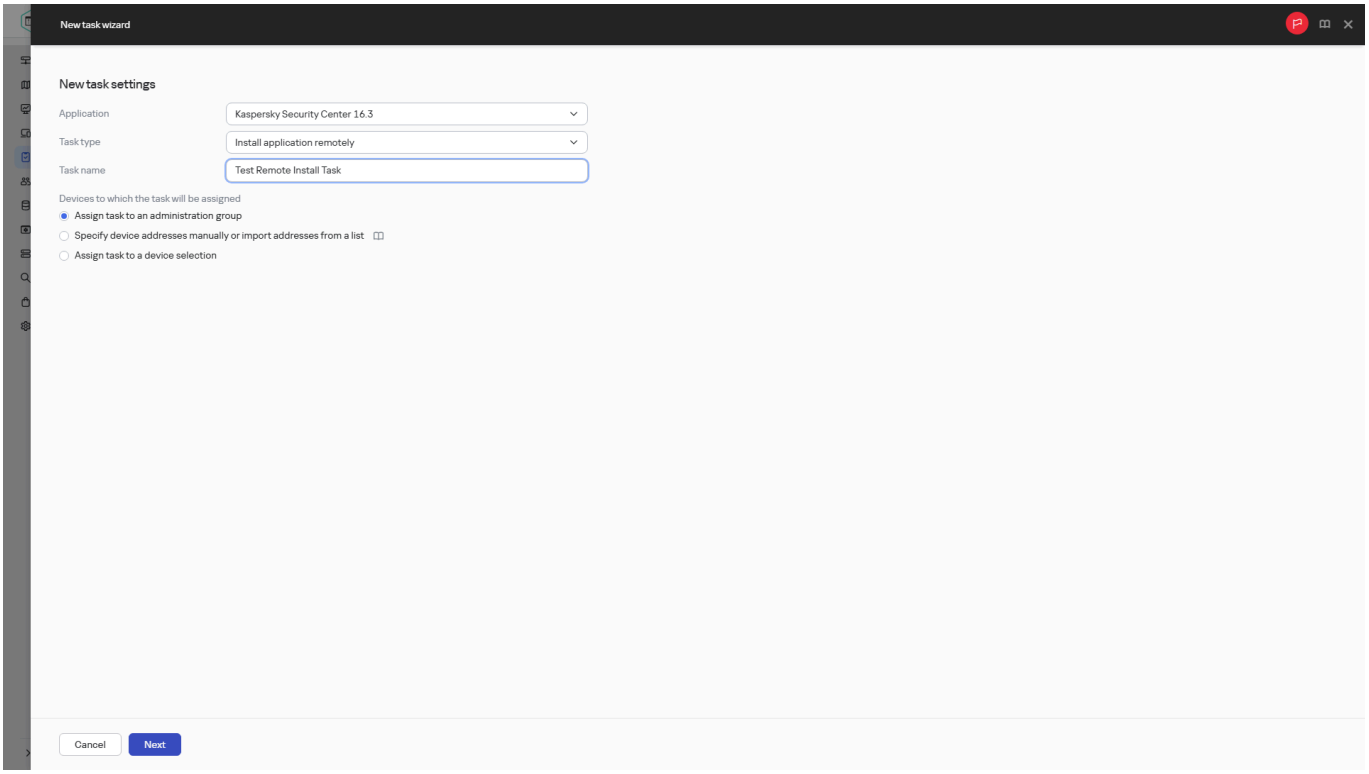
   Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

   Назначить задачу выборке устройств

   Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

   Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

Задача *Удаленная установка приложения* создана для указанных устройств. Если вы выбрали параметр **Назначить задачу группе администрирования**, задача является групповой.



Создание задачи Удаленная установка приложения

5. На шаге **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

   Доступные параметры зависят от параметра, выбранного на предыдущем шаге.

6. На шаге **Инсталляционные пакеты** укажите следующие параметры:

   - В поле **Выбор инсталляционного пакета** выберите инсталляционный пакет приложения, которое требуется установить.

   - В блоке параметров **Принудительно скачать инсталляционный пакет** выберите способ доставки на клиентские устройства файлов, необходимых для установки приложения:

     С помощью Агента администрирования

     Если этот параметр включен, доставку инсталляционных пакетов на клиентские устройства выполняет установленный на клиентских устройствах Агент администрирования.

     Если этот параметр выключен, инсталляционные пакеты доставляются с помощью инструментов операционной системы клиентского устройства.

     Рекомендуется включить этот параметр, если задача назначена для устройств с установленными Агентами администрирования.

     По умолчанию параметр включен.

     Средствами операционной системы с помощью точек распространения

     Если флажок установлен, инсталляционные пакеты передаются на клиентские устройства средствами операционной системы через агенты обновлений. Этот вариант можно выбрать, если в сети есть хотя бы один агент обновлений.

     Если установлен флажок **С помощью Агента администрирования**, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

По умолчанию флажок установлен для задач удаленной установки, созданных на виртуальном Сервере администрирования.

Единственный способ установить приложение для Windows (включая Агент администрирования для Windows) на устройство, на котором не установлен Агент администрирования, – это использовать точку распространения с операционной системой Windows. Поэтому при установке приложения для Windows:

- Выберите этот параметр.
- Убедитесь, что для целевых клиентских устройств назначена точка распространения.
- Убедитесь, что на точке распространения установлена операционная система Windows.

Средствами операционной системы с помощью Сервера администрирования

Если этот параметр включен, доставка файлов на клиентские устройства будет осуществляться средствами операционной системы клиентских устройств с помощью Сервера администрирования. Этот параметр можно включить, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

По умолчанию параметр включен.

- В поле **Максимальное количество одновременных загрузок** укажите максимально допустимое количество клиентских устройств, на которые Сервер администрирования может одновременно передавать файлы.
- В поле **Максимальное количество попыток установок** укажите максимально допустимое количество запусков приложения установки.

  Если количество попыток, указанное в параметрах задачи, превышено, Kaspersky Security Center Linux больше не запускает приложение установки на устройстве. Чтобы перезапустить задачу *Удаленная установка приложения*, увеличьте значение параметра **Максимальное количество попыток установок** и запустите задачу. Также вы можете создать другую задачу *Удаленная установка приложения*.
- Если вы переносите данные из одного приложения "Лаборатории Касперского" в другую, и ваше текущее приложение защищено паролем, введите пароль в поле **Пароль для удаления приложения "Лаборатории Касперского"**. Обратите внимание, что во время переноса данных ваше текущее приложение "Лаборатории Касперского" будет удалено.

  Поле **Пароль для удаления приложения "Лаборатории Касперского"** доступно, только если вы выбрали параметр **С помощью Агента администрирования** в группе параметров **Принудительно скачать инсталляционный пакет**.

  Вы можете использовать пароль деинсталляции только для сценария переноса данных Kaspersky Security для Windows Server в Kaspersky Endpoint Security для Windows при установке Kaspersky Endpoint Security для Windows с помощью задачи Удаленная установка приложений. Использование пароля деинсталляции при установке других компонентов может вызвать ошибки установки.

Для успешного завершения сценария переноса данных убедитесь, что выполнены следующие предварительные условия:

- Вы используете Агент администрирования Kaspersky Security Center версии 14.2 для Windows или выше.
- Вы устанавливаете приложение на устройства под управлением Windows.

- Настройте дополнительный параметр:

  Не устанавливать приложение, если оно уже установлено

  Если этот параметр включен, выбранное приложение не устанавливается заново, если оно уже установлено на клиентском устройстве.

  Если этот параметр выключен, приложение будет установлено в любом случае.

  По умолчанию параметр включен.

  Предварительно проверять тип операционной системы перед загрузкой

  Перед передачей файлов на клиентские устройства Kaspersky Security Center Linux проверяет, применимы ли параметры утилиты установки к операционной системе клиентского устройства. Если параметры не применимы, Kaspersky Security Center Linux не передает файлы и не пытается установить приложение. Например, чтобы установить некоторые приложения на устройства 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.

  При удаленной установке Агента администрирования на нераспределенные устройства Kaspersky Security Center Linux или точка распространения автоматически определяет тип операционной системы устройства независимо от параметра **Предварительно проверять тип операционной системы перед загрузкой**.

  Назначить установку инсталляционного пакета в групповых политиках Active Directory

  Если этот параметр включен, инсталляционный пакет будет устанавливаться с помощью групповых политик Active Directory.

  Параметр доступен, если выбран инсталляционный пакет Агента администрирования.

  По умолчанию параметр выключен.

  Предлагать пользователю закрыть работающие приложения

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.

- Выберите, на какие устройства вы хотите установить приложение:

  Устанавливать на все устройства

Приложение устанавливается даже на устройства, управляемые другими Серверами администрирования.

По умолчанию этот вариант выбран. Не нужно изменять этот параметр, если в вашей сети есть только один Сервер администрирования.

Устанавливать на устройства, управляемые только этим Сервером администрирования

Приложение устанавливается только на устройства, которые управляются данным Сервером администрирования. Выберите этот параметр, если в вашей сети установлено больше одного Сервера администрирования и вы хотите избежать конфликтов между ними.

- Укажите, следует ли перемещать устройства в группу администрирования после установки:

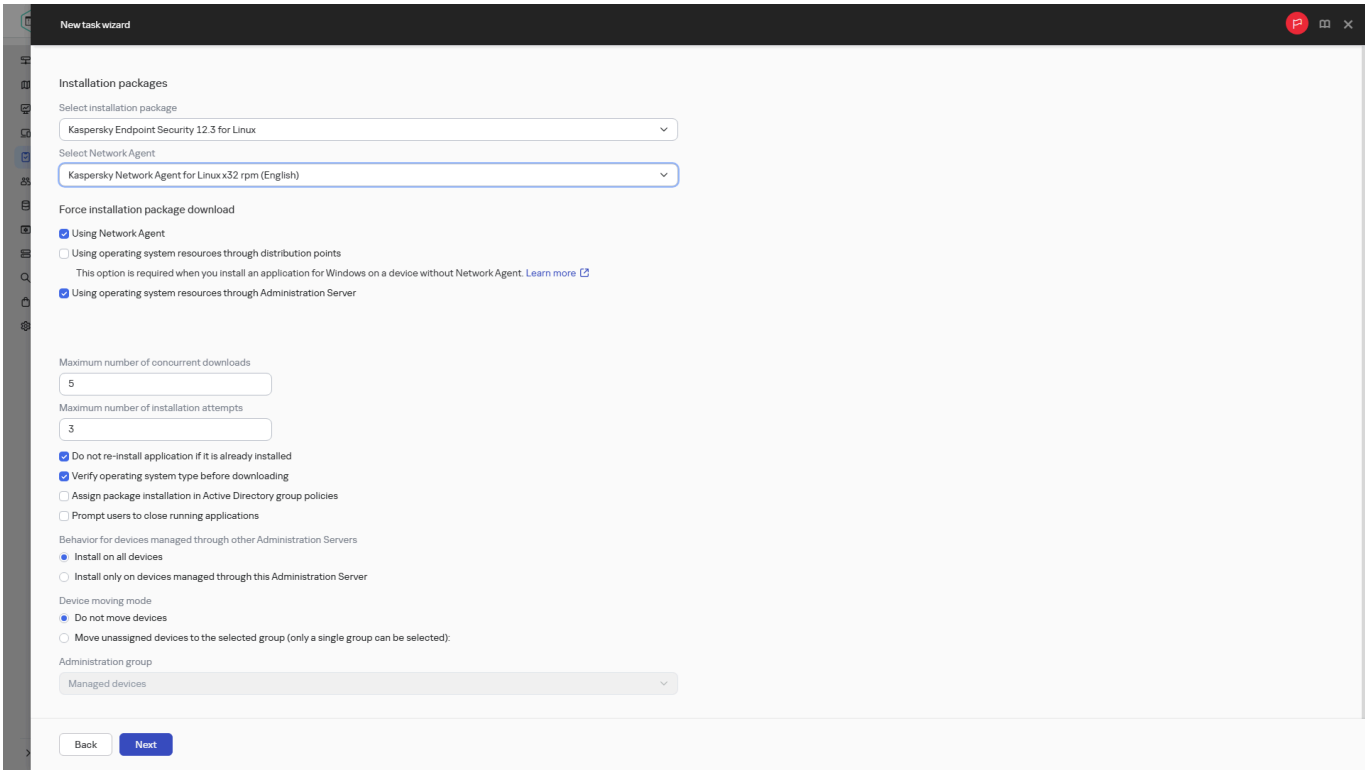
  Не перемещать устройства

  Устройства остаются в тех группах, к которым они принадлежат. Устройства, не принадлежащие ни к одной из групп, остаются нераспределенными.

  Переместить нераспределенные устройства в выбранную группу (можно выбрать только одну группу)

  Устройства перемещаются в выбранную вами группу администрирования.

  Обратите внимание, что по умолчанию выбран вариант **Не перемещать устройства**. По соображениям безопасности вы можете предпочесть перемещение устройств вручную.



Указание параметров задачи

7. На этом шаге мастера укажите, требуется ли перезагрузка устройства при установке приложений:

   Не перезагружать устройство

   Если выбран этот вариант, устройство не будет перезагружаться после установки приложения безопасности.

   Перезагрузить устройство

   Если выбран этот вариант, устройство будет перезагружено после установки приложения безопасности.

8. При необходимости на шаге **Выбор учетных записей для доступа к устройствам** добавьте учетные записи, которые будут использоваться для запуска задачи *Удаленная установка приложения*.

   Учетная запись не требуется (Агент администрирования уже установлен)

   Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор приложения. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

   Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

   Учетная запись требуется (Агент администрирования не используется)

   Выберите этот вариант, если Агент администрирования не установлен на устройствах, для которых вы назначаете задачу удаленной установки. В этом случае вы можете указать учетную запись пользователя или SSH-сертификат для установки приложения.

   - **Локальная или доменная учетная запись**. Если выбран этот вариант, укажите учетную запись пользователя, от имени которой будет запускаться установщик приложения. Нажмите на кнопку **Добавить**, выберите **Локальная или доменная 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 приложение 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 Linux поддерживает формат закрытых ключей PEM, а утилита ssh-keygen по умолчанию генерирует SSH-ключи в формате OPENSSH. Формат OPENSSH не поддерживается Kaspersky Security Center Linux. 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>"
     ```

9. На шаге **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

   Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи. В этом окне можно проверить параметры задачи, изменить их или при необходимости настроить расписание запуска задачи.

10. В списке задач выберите созданную задачу и нажмите на кнопку **Запустить**.

    Или дождитесь запуска задачи в соответствии с расписанием, указанным в параметрах задачи.

После выполнения задачи удаленной установки, выбранное приложение устанавливается на указанный набор устройств.

Удаленная установка приложений на устройства с операционной системой macOS

Чтобы установить приложения на устройства с операционной системой macOS с помощью задачи удаленной установки:

1. Создайте архив, состоящий из инсталляционного пакета и установочного скрипта .sh.

2. Выключите параметр **Предварительно проверять тип операционной системы перед загрузкой** в мастере создания задачи.

Также вы можете использовать задачу **Удаленное выполнение скриптов**. В следующей статье описывается, как настроить файлы для этой задачи: Удаленная установка приложений на устройства с помощью задачи Удаленное выполнение скриптов.

Установка приложений на подчиненные Серверы администрирования

Если у вас версия Сервера администрирования 15.4 или выше, вы можете устанавливать приложения на подчиненный Сервер администрирования только в том случае, если его версия 15.4 или выше.

Чтобы установить приложение на подчиненные Серверы администрирования:

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.

2. Убедитесь в том, что соответствующий устанавливаемому приложению инсталляционный пакет находится на каждом из выбранных подчиненных Серверов администрирования. Если вы не можете найти инсталляционный пакет ни на одном из подчиненных Серверов, распространите его. Для этого создайте задачу с типом задачи **Распространение инсталляционного пакета**.

3. Создайте задачу удаленной установки приложения на подчиненных Серверах администрирования. Выберите тип задачи **Удаленная установка приложения на подчиненный Сервер администрирования**.

   В результате работы мастера создания задачи будет создана задача удаленной установки выбранного приложения на выбранные подчиненные Серверы администрирования.

4. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

После выполнения задачи удаленной установки выбранное приложение устанавливается на подчиненные Серверы администрирования.

Удаленная установка приложений на устройства с установленным Агентом администрирования

Если на устройстве установлен работоспособный Агент администрирования, подключенный к главному Серверу администрирования или к одному из его подчиненных Серверов, то на этом устройстве можно обновлять версию Агента администрирования, а также устанавливать, обновлять или удалять с помощью Агента администрирования любые поддерживаемые приложения.

Эта функция включается параметром **С помощью Агента администрирования** в свойствах задачи удаленной установки приложений.

Если параметр выбран, то передача на устройства инсталляционных пакетов с заданными администратором инсталляционными параметрами осуществляется по каналам связи между Агентом администрирования и Сервером администрирования.

Для оптимизации нагрузки на Сервер администрирования и минимизации трафика между Сервером администрирования и устройствами целесообразно назначать в каждой удаленной сети или в каждом широковещательном домене точки распространения (см. разделы "О точках распространения" и "Построение структуры групп администрирования и назначение точек распространения"). В этом случае распространение инсталляционных пакетов и параметров инсталлятора осуществляется с Сервера администрирования на устройства через точки распространения.

Также с использованием точек распространения можно выполнять широковещательную (многоадресную) рассылку инсталляционных пакетов, что позволяет многократно снизить сетевой трафик в ходе развертывания приложений.

При передаче инсталляционных пакетов на устройства по каналам связи между Агентами администрирования и Сервером администрирования подготовленные к передаче инсталляционные пакеты дополнительно кешируются в папке /var/opt/kaspersky/klnagent_srv/1093/.working/. При использовании большого числа различных инсталляционных пакетов большого размера и при большом количестве точек распространения размер этой папки может существенно увеличиваться.

Удалять файлы из папки FTServer вручную невозможно. При удалении исходных инсталляционных пакетов соответствующие данные будут автоматически удаляться и из папки FTServer.

Данные, принимаемые точками распространения, сохраняются в папке /var/opt/kaspersky/klnagent_srv/1103/.

Удалять файлы из папки $FTCITmp вручную невозможно. По мере завершения задач, использующих данные из папки, содержимое этой папки будет удаляться автоматически.

Поскольку инсталляционные пакеты распространяются по каналам связи между Сервером администрирования и Агентами администрирования из промежуточного хранилища в оптимизированном для передачи по сети формате, невозможно вносить изменения в инсталляционные пакеты в исходной папке инсталляционного пакета. Такие изменения не будут автоматически учтены Сервером администрирования. Если необходимо изменить вручную файлы инсталляционных пакетов (хотя делать это не рекомендуется), нужно обязательно изменить какие-либо параметры инсталляционного пакета в Kaspersky Security Center Web Console. Изменение параметров инсталляционного пакета в Kaspersky Security Center Web Console заставит Сервер администрирования обновить образ пакета в кеше, подготовленном для передачи на устройства.

Сервер отправляет эхо-запросы ICMP (такие же, как и команда ping) на целевое устройство во время удаленной установки.

Управление перезагрузкой устройств в задаче удаленной установки

Часто для завершения удаленной установки приложений (особенно на платформе Windows) требуется перезагрузка устройства.

Если используется задача удаленной установки приложений Kaspersky Security Center Linux, в мастере создания задачи или в окне свойств созданной задачи (раздел **Перезагрузка операционной системы**) можно выбрать вариант действия при необходимости перезагрузки:

- **Не перезагружать устройство**. В этом случае автоматическая перезагрузка не будет выполнена. Для завершения установки потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки будет сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач установки на серверы и другие устройства, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**. В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения установки. Этот вариант подходит для задач установки на устройства, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**. На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Вариант **Запрашивать у пользователя** наиболее подходит для рабочих станций, пользователи которых должны иметь возможность выбрать наиболее подходящий момент для перезагрузки.

Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center Linux

Для того чтобы выполнить первоначальное развертывание Агента администрирования или других приложений, вы можете принудительно установить выбранные инсталляционные пакеты с помощью задачи удаленной установки Kaspersky Security Center Linux при условии, что на каждом устройстве есть учетные записи пользователей с правами локального администратора.

Принудительная установка может быть использована и в случае, если устройства не доступны Серверу администрирования непосредственно: например, устройства расположены в изолированных сетях, или устройства расположены в локальной сети, а Сервер администрирования – в демилитаризованной зоне.

В случае первоначального развертывания Агент администрирования не устанавливается. Поэтому в параметрах задачи удаленной установки невозможно выбрать распространение файлов, необходимых для установки приложения с помощью Агента администрирования. Вы можете распространять файлы, только используя ресурсы операционной системы с помощью Сервера администрирования или точек распространения.

Служба Сервера администрирования должна запускаться под учетной записью, имеющей права администратора на целевых устройствах. Также вы можете указать учетную запись, имеющую доступ к административным ресурсам общего доступа admin$, в параметрах задачи удаленной установки.

По умолчанию задача удаленной установки применяется к устройствам и использует учетные данные учетной записи, под которой запущен Сервер администрирования. Обратите внимание, что это учетная запись, используемая для доступа к административным ресурсам общего доступа admin$, а не учетная запись, под которой выполняется задача удаленной установки. Установка выполняется под учетной записью LocalSystem.

Вы можете указать целевые устройства явно (списком), выбрав группу администрирования Kaspersky Security Center Linux, которой они принадлежат, или создав выборку устройств по определенному условию. Время запуска установки определяется расписанием задачи. Если в свойствах задачи включен параметр **Запускать пропущенные задачи**, задача может запускаться сразу при включении устройств или при переносе их в целевую группу администрирования.

Принудительная установка осуществляется путем доставки инсталляционных пакетов на целевые устройства, последующего копирования файлов на административный ресурс admin$ каждого из устройств и удаленной регистрации на них вспомогательных служб. Рассылка инсталляционных пакетов на целевые устройства выполняется с помощью функции Kaspersky Security Center Linux, отвечающей за сетевое взаимодействие. При этом должны выполняться следующие условия:

- Целевые устройства доступны со стороны Сервера администрирования или со стороны точки распространения.
- В сети корректно работает разрешение имен для устройств.
- На целевых устройствах включены административные ресурсы общего доступа admin$.
- На целевых устройствах запущены следующие системные службы:
  - Сервер (LanmanServer).

    По умолчанию эта служба запущена.
  - DCOM Server Process Launcher (DcomLaunch).
  - RPC Endpoint Mapper (RpcEptMapper).
  - Вызов удаленной процедуры (Remote Procedure Call, RpcSs).
- TCP-порт 445 открыт на целевых устройствах для обеспечения удаленного доступа с помощью инструментария управления Windows (WMI).

  TCP 139, UDP 137 и UDP 138 используются старыми протоколами и больше не нужны для текущих приложений.

  На сетевом экране должны быть разрешены динамические исходящие порты доступа для соединения Сервера администрирования и точек распространения с целевыми устройствами.
- В параметрах безопасности политики домена Active Directory разрешено обеспечивать работу NTLM-протокола при развертывании Агента администрирования.
- На целевых устройствах под управлением Microsoft Windows XP режим Simple File Sharing выключен.

- На целевых устройствах настроена модель совместного доступа и безопасности *Классическая – локальные пользователи выполняют аутентификацию самих себя*. Такая модель не может быть *Только гостевой – локальные пользователи выполняют аутентификацию как Гость*.

- Устройства являются членами домена, либо на устройствах заблаговременно созданы унифицированные учетные записи с административными правами.

Чтобы успешно развернуть Агент администрирования или другие приложения на устройстве, не подключенном к домену Active Directory с версией операционной системы Windows Server 2003 и выше, необходимо выключить удаленный UAC на этом устройстве. Удаленный UAC – это одна из причин, по которой учетные записи локальных администраторов не могут получить доступ к admin$, который требуется для принудительного развертывания Агента администрирования и других приложений. Выключение удаленного UAC не влияет на локальный UAC.

При установке на новые устройства, еще не размещенные в группах администрирования Kaspersky Security Center Linux, в свойствах задачи удаленной установки можно задать группу администрирования, в которую устройства будут перемещаться по завершении установки на них Агента администрирования.

При создании групповой задачи необходимо помнить, что групповая задача действует на устройства всех вложенных подгрупп выбранной группы. Поэтому не следует дублировать задачи установки в подгруппах.

Упрощенным способом создания задач для принудительной установки приложений является автоматическая установка. Для этого в свойствах группы администрирования вам нужно открыть список инсталляционных пакетов и выбрать те пакеты, которые должны быть установлены на устройствах этой группы. В результате на всех устройствах этой группы и ее подгрупп будут автоматически установлены выбранные инсталляционные пакеты. Период, в течение которого будут установлены пакеты, зависит от пропускной способности сети и общего количества устройств в сети.

Чтобы снизить нагрузку на Сервер администрирования при распространении инсталляционных пакетов на целевые устройства, вы можете выбрать установку с помощью точек распространения в задаче установки. Следует учитывать, что данный способ установки создает значительную нагрузку на устройства, назначенные точками распространения. Рекомендуется выбирать устройства, соответствующие требованиям для точек распространения. Если вы используете точки распространения, вам нужно убедиться, что они присутствуют в каждой из изолированных подсетей, на которых размещены целевые устройства.

Использование точек распространения в качестве локальных центров установки может быть удобно и для установки на устройства в подсетях, соединенных с Сервером администрирования узким каналом связи при наличии широкого канала связи между устройствами внутри подсети.

Объем свободного места в разделе с папкой /var/opt/kaspersky/KSC_Backups* должен многократно превосходить суммарный объем дистрибутивов устанавливаемых приложений.

Установка приложений в тихом режиме

Чтобы установить приложение в тихом режиме:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Инсталляционные пакеты**.

2. Установите флажок рядом с инсталляционным пакетом нужного приложения или создайте инсталляционный пакет для этого приложения.

   Инсталляционный пакет будет сохранен на Сервере администрирования в папке общего доступа в служебной папке Packages. При этом каждому инсталляционному пакету соответствует отдельная вложенная папка.

3. Откройте папку нужного инсталляционного пакета одним из следующих способов:

   - Скопируйте папку, соответствующую нужному инсталляционному пакету, с Сервера администрирования на клиентское устройство. Затем откройте скопированную папку на клиентском устройстве.

   - С клиентского устройства откройте на Сервере администрирования папку общего доступа, соответствующую нужному инсталляционному пакету.

   Если папка общего доступа расположена на устройстве с установленной операционной системой Microsoft Windows Vista, необходимо установить значение **Выключено** для параметра **Управление учетными записями пользователей: все администраторы работают в режиме одобрения администратором** (**Пуск** → **Панель управления** → **Администрирование** → **Локальная политика безопасности** → **Параметры безопасности**).

4. В зависимости от выбранного приложения выполните следующие действия:

   - Для Антивируса Касперского для Windows Workstations, Антивируса Касперского для Windows Servers и Kaspersky Security Center перейдите во вложенную папку exec и запустите исполняемый файл (файл с расширением exe) с ключом /s.

   - Для остальных приложений "Лаборатории Касперского" запустите из открытой папки исполняемый файл (файл с расширением exe) с ключом /s.

   Запуск исполняемого файла с ключами `EULA=1` и `PRIVACYPOLICY=1` означает, что вы полностью прочитали, поняли и принимаете положения Лицензионного соглашения и Политики конфиденциальности соответственно. Вам также известно, что ваши данные будут обрабатываться и передаваться (в том числе в третьи страны), как описано в Политике конфиденциальности. Текст Лицензионного соглашения и текст Политики конфиденциальности входят в комплект поставки Kaspersky Security Center Linux. Согласие с положениями Лицензионного соглашения и Политики конфиденциальности является необходимым условием для установки приложения или обновления предыдущей версии приложения.

Подготовка устройства с операционной системой macOS к удаленной установке Агента администрирования

Предусмотрены следующие способы первоначальной установки Агента администрирования на управляемое устройство с операционной системой macOS:

- Запустить задачу удаленной установки на точке распространения с операционной системой macOS.
- Отправить пользователям устройств ссылки на автономные пакеты, сформированные Kaspersky Security Center Linux. Автономные пакеты представляют собой исполняемые модули, содержащие в себе дистрибутивы выбранных приложений с настроенными параметрами.

Чтобы подготовить устройство с операционной системой macOS к удаленной установке Агента администрирования:

1. Убедитесь, что на целевом устройстве с операционной системой macOS установлено приложение sudo.
2. Выполните проверку конфигурации устройства:
   a. Убедитесь, что порт 22 открыт на клиентском устройстве. Для этого в разделе **Системные настройки** откройте панель **Обмен** и убедитесь, что установлен флажок **Удаленный вход**.

      Вы можете подключиться к клиентскому устройству по протоколу Secure Shell (SSH) только через порт 22. Вы не можете изменить номер порта.

      Вы можете использовать команду `ssh <device_name>` для удаленного входа на устройство macOS. В панели **Общий доступ** можно использовать параметр **Разрешить доступ для** чтобы задать область действия пользователей, которым разрешен доступ к устройству macOS.

   b. Отключите пароль запроса sudo для учетной записи пользователя, которая используется для подключения к устройству.

      Используйте команду `sudo visudo`, чтобы открыть конфигурационный файл sudoers в терминале. В файле, который вы открыли, в поле `User privilege specification` укажите следующее: `username ALL = (ALL) NOPASSWD: ALL`. В этом случае `username` является учетной записью пользователя, которая будет использоваться для подключения к устройству по протоколу SSH.

   c. Сохраните и закройте файл sudoers.

   d. Повторно подключитесь к устройству через SSH и проверьте, что служба sudo не требует пароль, с помощью команды `sudo whoami`.

3. Загрузите и создайте инсталляционный пакет:
   a. Загрузите инсталляционный пакет Агента администрирования одним из следующих способов:
      - Используя интерфейс приложения.
      - Загрузив соответствующую версию Агента администрирования с веб-сайта Службы технической поддержки по адресу https://support.kaspersky.ru/.
      - Запросив инсталляционный пакет у специалистов Службы технической поддержки.

b. Для создания пакета удаленной установки используйте файлы:

- klnagent.kud
- install.sh
- klnagentmac.dmg

4. Создайте задачу удаленной установки приложения с параметрами:

- В окне **Параметры** мастера создания задачи установите флажок **Средствами операционной системы с помощью Сервера администрирования**. Снимите все остальные флажки.
- В окне **Выбор учетной записи для запуска задачи** для запуска задачи укажите параметры учетной записи, которая используется для подключения к устройству через SSH.

Клиентское устройство готово к удаленной установке Агента администрирования с помощью соответствующей задачи, которую вы создали.

Виртуальная инфраструктура

Kaspersky Security Center Linux поддерживает работу с виртуальными машинами. Вы можете установить Агент администрирования и приложения безопасности на каждую виртуальную машину, а также вы можете защищать виртуальные машины на уровне гипервизора. В первом случае для защиты виртуальных машин можно использовать как обычное приложение безопасности, так и Kaspersky Security для виртуальных сред Легкий агент. Во втором случае вы можете использовать Kaspersky Security для виртуальных сред Защита без агента.

Kaspersky Security Center Linux поддерживает откат виртуальных машин к предыдущему состоянию.

Рекомендации по снижению нагрузки на виртуальные машины

В случае инсталляции Агента администрирования на виртуальную машину следует рассмотреть возможность отключения той части функциональности Kaspersky Security Center Linux, которая не очень полезна для виртуальных машин.

При установке Агента администрирования на виртуальную машину или на шаблон, из которого в дальнейшем будут получены виртуальные машины, рекомендуется выполнить следующие действия:

- если выполняется удаленная установка, в окне свойств инсталляционного пакета Агента администрирования (в разделе **Дополнительно**) выбрать параметр **Оптимизировать параметры для VDI**;
- если выполняется интерактивная установка с помощью мастера, в окне мастера выбрать параметр **Оптимизировать параметры Агента администрирования для виртуальной инфраструктуры**.

Выбор параметров изменит параметры Агента администрирования таким образом, чтобы по умолчанию (до применения политики) были выключены следующие функции:

- получение информации об установленном программном обеспечении;
- получение информации об аппаратном обеспечении;

- получение информации о наличии уязвимостей;
- получение информации о необходимых обновлениях.

Как правило, перечисленные функции не нужны на виртуальных машинах в силу того, что программное обеспечение и виртуальное аппаратное обеспечение на них единообразны.

Выключение функций обратимо. Если любая из выключенных функций все же нужна, ее можно включить при помощи политики Агента администрирования, или в локальных параметрах Агента администрирования. Локальные параметры Агента администрирования доступны из контекстного меню соответствующего устройства в Kaspersky Security Center Web Console.

Поддержка динамических виртуальных машин

Kaspersky Security Center Linux поддерживает динамические виртуальные машины. Если в сети организации развернута виртуальная инфраструктура, то в некоторых случаях могут использоваться динамические (временные) виртуальные машины. Такие машины создаются с уникальными именами из заранее подготовленного администратором шаблона. Пользователь работает с созданной машиной некоторое время, а после выключения виртуальная машина удаляется из виртуальной инфраструктуры. Если в сети организации развернут Kaspersky Security Center Linux, то виртуальная машина с установленным на ней Агентом администрирования добавляется в базу данных Сервера администрирования. После выключения виртуальной машины запись о ней должна быть также удалена и из базы данных Сервера администрирования.

Чтобы функциональность автоматического удаления записей о виртуальных машинах работала, при установке Агента администрирования на шаблон, из которого будут созданы динамические виртуальные машины, нужно выбрать параметр **Включить динамический режим для VDI**:

- в случае удаленной установки – в окне свойств инсталляционного пакета Агента администрирования (раздел **Дополнительно**);
- в случае интерактивной установки – в мастере установки Агента администрирования.

Параметр **Включить динамический режим для VDI** не следует выбирать при установке Агента администрирования на физические устройства.

Если нужно, чтобы события с динамических виртуальных машин сохранялись на Сервере администрирования некоторое время после удаления машин, то следует в окне свойств Сервера администрирования в разделе **Хранилище событий** выбрать параметр **Хранить события после удаления устройств** и указать максимальное время хранения событий в днях.

Не рекомендуется включать шифрование дисков на динамических виртуальных машинах.

Поддержка копирования виртуальных машин

Копирование виртуальной машины с установленным на нее Агентом администрирования или ее создание из шаблона с установленным Агентом администрирования эквивалентно развертыванию Агентов администрирования захватом и копированием образа жесткого диска. Поэтому в общем случае при копировании виртуальных машин нужно выполнять те же действия, что и при развертывании копированием образа диска.

Однако в описанных ниже двух случаях Агент администрирования обнаруживает факт копирования автоматически. Поэтому выполнять сложные действия, описанные в разделе "Развертывание захватом и копированием жесткого диска устройства", необязательно:

- При установке Агента администрирования был выбран параметр **Включить динамический режим для VDI**: после каждой перезагрузки операционной системы такая виртуальная машина будет считаться новым устройством, независимо от факта ее копирования.
- Используется один из следующих гипервизоров: VMware™, HyperV® или Xen®: Агент администрирования определит факт копирования виртуальной машины по изменившимся идентификаторам виртуального аппаратного обеспечения.

Анализ изменений виртуального аппаратного обеспечения не абсолютно надежен. Прежде чем широко использовать данный метод, следует предварительно проверить его работоспособность на небольшом количестве виртуальных машин для используемой в организации версии гипервизора.

Указание параметров удаленной установки на устройствах под управлением Unix

Когда вы устанавливаете приложение на устройство под управлением Unix с помощью задачи удаленной установки, вы можете указать параметры, специфичные для Unix, для этой задачи. Эти параметры доступны в свойствах задачи после ее создания.

Чтобы указать параметры, специфичные для Unix, для задачи удаленной установки:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на название задачи удаленной установки, для которой вы хотите указать параметры, специфичные для Unix.

   Откроется окно свойств задачи.
3. Перейдите в раздел **Параметры приложения → Параметры, специфичные для Unix**.
4. Задайте следующие параметры:

   Установить пароль для учетной записи root (только для развертывания через SSH)

Если команду `sudo` невозможно использовать на целевом устройстве без указания пароля, выберите этот параметр, а затем укажите пароль для учетной записи root. Kaspersky Security Center 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 Linux не использует учетную запись или указанный пароль для создания SSH-соединения.

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 Linux использует указанную папку в качестве временной папки для доступа по SSH. Приложение помещает инсталляционный пакет в директорию и запускает процедуру установки.

5. Нажмите на кнопку **Сохранить**.

Указанные параметры задачи сохранены.

Мониторинг развертывания

Чтобы контролировать развертывание Kaspersky Security Center Linux и убедиться, что приложение безопасности и Агент администрирования установлены на управляемых устройствах, используйте функции мониторинга и отчеты:

- Используйте виджет развертывания в панели инструментов для мониторинга развертывания в режиме реального времени.
- Используйте отчеты, чтобы получить подробную информацию.

Запуск и остановка приложений "Лаборатории Касперского"

Вы можете использовать задачу *Запуск или остановка приложения* для запуска и остановки приложений "Лаборатории Касперского" на управляемых устройствах.

Чтобы создать задачу запуска или остановки приложения:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В раскрывающемся списке **Приложение** выберите приложение, для которого вы хотите создать задачу.

   Приложения "Лаборатории Касперского" отображаются в списке, если вы ранее добавили веб-плагины управления этих приложений.

4. В списке **Тип задачи** выберите задачу **Активация приложения**.

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 **Приложения** выполните следующее:

   - Установите флажки рядом с названиями приложений, для которых вы хотите создать задачу.
   - Выберите параметр **Запустить приложение** или **Остановить приложение**.

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 приложений безопасности сторонних производителей

Для установки приложения безопасности "Лаборатории Касперского" средствами Kaspersky Security Center Linux может потребоваться удалить приложение стороннего производителя, несовместимое с устанавливаемым приложением. Kaspersky Security Center Linux предоставляет несколько способов удаления приложений сторонних производителей.

Удаление несовместимых приложений при настройке удаленной установки приложения

Вы можете включить параметр **Удалять несовместимые приложения автоматически** во время настройки удаленной установки приложения безопасности в мастере развертывания защиты. Если этот параметр включен, Kaspersky Security Center Linux удаляет несовместимые приложения перед установкой приложения безопасности на управляемое устройство.

Удаление несовместимых приложений с помощью отдельной задачи

Для удаления несовместимых приложений используется задача *Удаленная деинсталляция приложения*. Задачу следует запускать на устройствах перед задачей установки приложения безопасности. Например, в задаче установки можно выбрать расписание типа **По завершении другой задачи**, где другой задачей является задача *Удаленная деинсталляция приложения*.

Этот способ удаления целесообразно использовать в случаях, если инсталлятор приложения безопасности не может успешно удалить какое-либо из несовместимых приложений.

Удаленная деинсталляция приложений или обновлений программного обеспечения

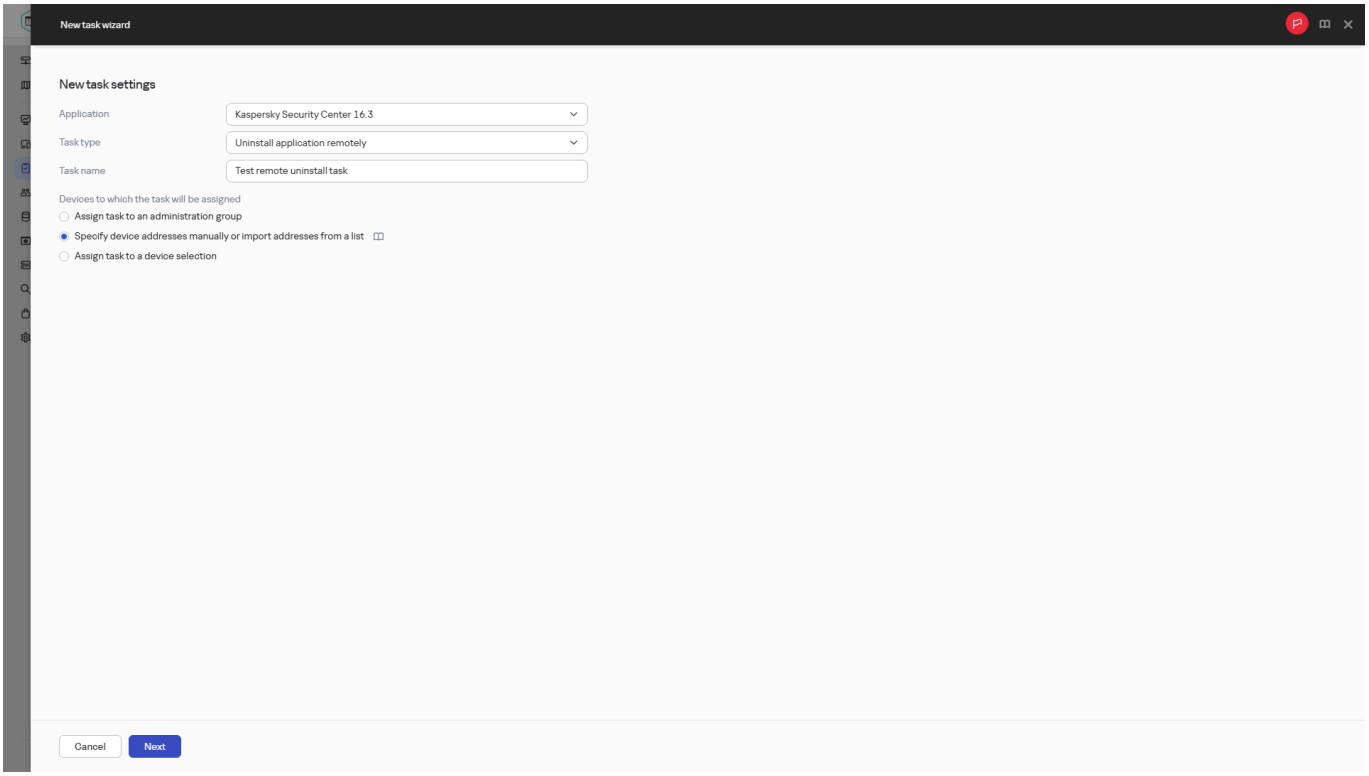
Вы можете удаленно деинсталлировать приложения или обновления программного обеспечения на управляемых устройствах под управлением Linux только с помощью Агента администрирования.

Чтобы удаленно деинсталлировать приложения или обновления программного обеспечения:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится Мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В раскрывающемся списке **Приложение** выберите Kaspersky Security Center Linux.
4. В списке **Тип задачи** выберите тип задачи **Удаленная деинсталляция приложения**.
5. В поле **Название задачи** укажите название новой задачи.

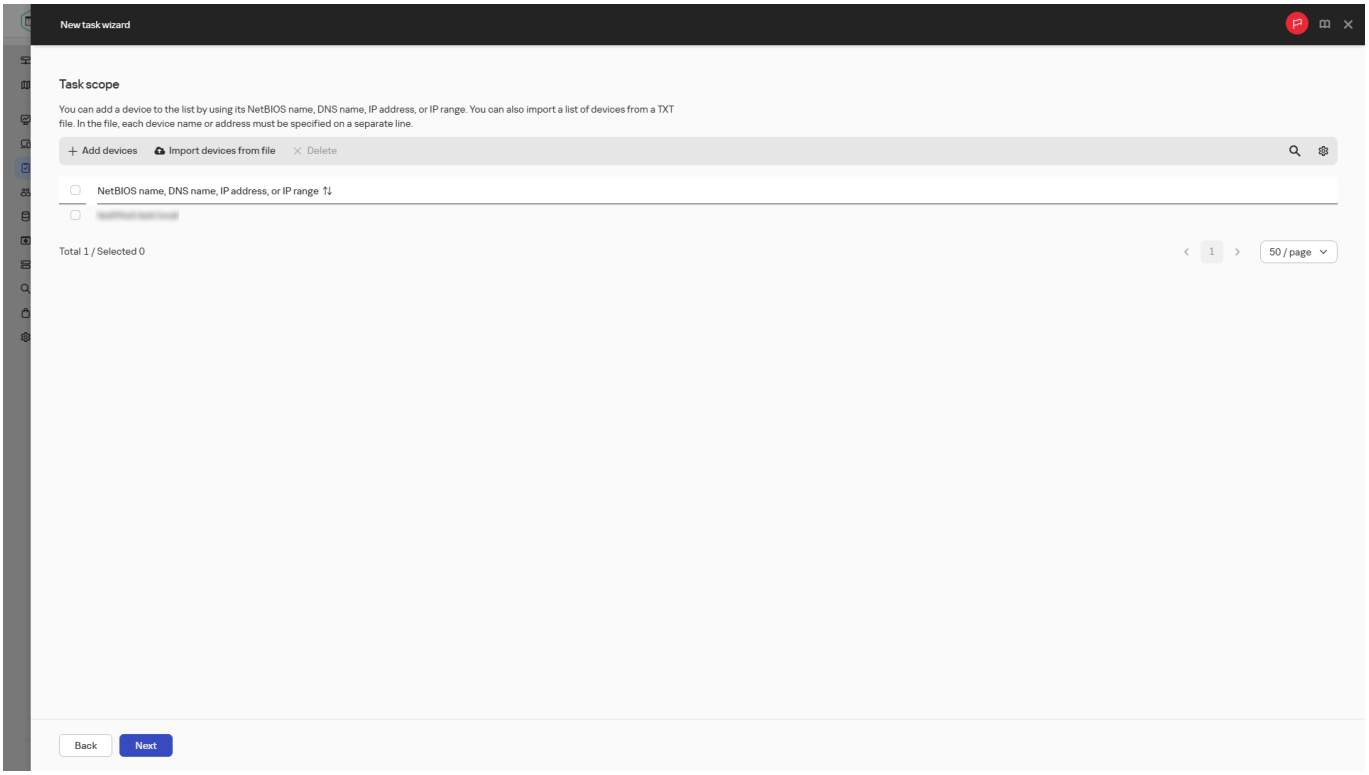
Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).



Создание задачи Удаленная деинсталляция приложения

6. Выберите устройства, которым будет назначена задача.

   Перейдите к следующему шагу мастера.



Указание области действия задачи

7. Выберите, какое приложение вы хотите деинсталлировать, а затем выберите требуемые приложения, обновления или патчи, которые вы хотите удалить:

   Удалить управляемое приложение

Отображается список приложений "Лаборатории Касперского". Выберите приложение, которое вы хотите деинсталлировать.

Удалить несовместимое приложение

Отобразится список приложений, несовместимых с приложениями безопасности "Лаборатории Касперского" или с Kaspersky Security Center Linux. Установите флажки напротив приложений, которые требуется удалить.

Удалить приложение из реестра приложений

По умолчанию Агенты администрирования отправляют на Сервер администрирования информацию о приложениях, установленных на управляемых устройствах. Список установленных приложений хранится в реестре приложений.

Чтобы выбрать приложение из реестра приложений:

a. Нажмите на поле **Приложение для деинсталляции** и выберите приложение, которое 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 приложение:

  - **Автоматически определять команду удаления**

    Если у приложения есть команда деинсталляции, заданная поставщиком приложения, Kaspersky Security Center Linux использует эту команду. Рекомендуется выбрать этот вариант.

  - **Задать команду удаления**

    Выберите этот вариант, если вы хотите указать свою команду для деинсталляции приложения.

    > Рекомендуется сначала попробовать деинсталлировать приложение 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 Linux проверяет, есть ли у выбранного приложения команда деинсталляции, заданная поставщиком приложения. Если команда найдена, Kaspersky Security Center Linux будет использовать ее вместо команды, указанной в поле **Команда для удаления приложения**.

    Рекомендуется включать этот параметр.

- **Выполнить перезагрузку после успешного удаления приложения**

  Если после деинсталляции приложения требуется перезагрузка операционной системы на управляемом устройстве, операционная система перезагружается автоматически.

Удалить указанное обновление приложения, патч или стороннее приложение

Отображается список обновлений, патчей и приложений сторонних производителей. Выберите объект, который вы хотите деинсталлировать.

Отображаемый список представляет собой общий список приложений и обновлений, и он не соответствует приложениям и обновлениям, установленным на управляемых устройствах. Перед выбором объекта рекомендуется убедиться, что приложение или обновление установлено на устройствах, определенных в области действия задачи. В окне свойств можно просмотреть список устройств, на которых установлено приложение или обновление.

Чтобы просмотреть список устройств:

a. Нажмите на имя приложения или обновления.

   Откроется окно свойств.

b. Откройте раздел **Устройства**.

   Вы также можете просмотреть список установленных приложений и обновлений в окне свойств устройства.

8. 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 деинсталлировано приложение, но нагрузка на Сервер администрирования увеличивается.

Максимальное количество попыток деинсталляции

Если при запуске задачи *Удаленная деинсталляция приложения* Kaspersky Security Center Linux не удается деинсталлировать приложение с управляемого устройства за указанное в параметрах количество запусков установок, Kaspersky Security Center Linux 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.

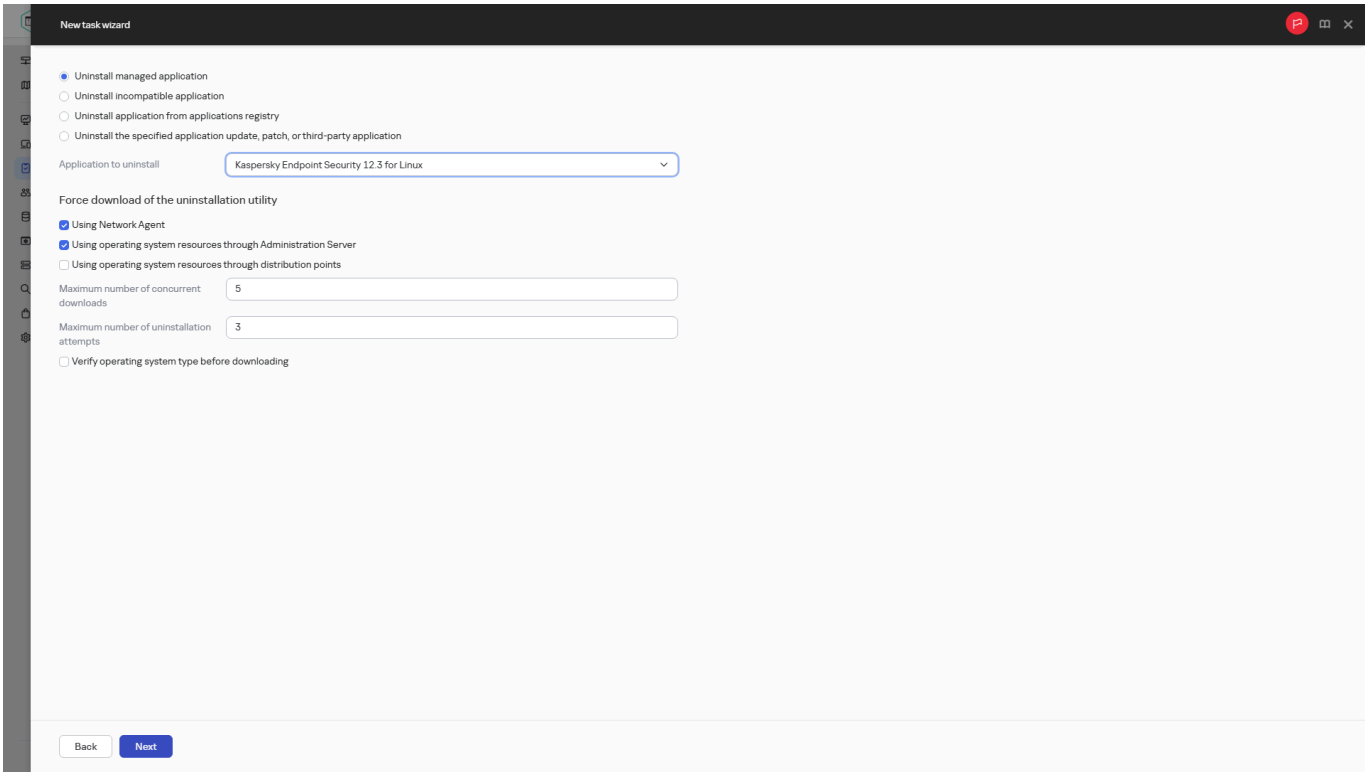
Если количество попыток деинсталляции, указанное в параметрах задачи, было превышено и устройство готово к деинсталляции приложения, вы можете увеличить значение параметра **Максимальное количество попыток деинсталляции** и запустить задачу деинсталляции приложения. Также вы можете создать другую задачу *Удаленная деинсталляция приложения*.

Предварительно проверять тип операционной системы перед загрузкой

Перед передачей файлов на клиентские устройства Kaspersky Security Center Linux проверяет, применимы ли параметры утилиты установки к операционной системе клиентского устройства. Если параметры не применимы, Kaspersky Security Center Linux не передает файлы и не пытается установить приложение. Например, чтобы установить некоторые приложения на устройства 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.

При удаленной установке Агента администрирования на нераспределенные устройства Kaspersky Security Center Linux или точка распространения автоматически определяет тип операционной системы устройства независимо от параметра **Предварительно проверять тип операционной системы перед загрузкой**.

Перейдите к следующему шагу мастера.



Указание параметров задачи

9. Укажите параметры перезагрузки операционной системы:

Не перезагружать устройство

Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

Перезагрузить устройство

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

Запрашивать у пользователя

На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**
- **Принудительно перезагрузить через (мин)**

Принудительно закрывать приложения в заблокированных сеансах

Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

Перейдите к следующему шагу мастера.

10. Если необходимо, добавьте учетные записи, которые будут использоваться для запуска задачи удаленной деинсталляции:

    Учетная запись не требуется (Агент администрирования уже установлен)

    Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор приложения. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

    Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

    Учетная запись требуется (Агент администрирования не используется)

    Выберите этот вариант, если Агент администрирования не установлен на устройствах, для которых вы назначаете задачу *Удаленная деинсталляция приложения*. В этом случае вы можете указать учетную запись пользователя или SSH-сертификат для деинсталляции приложения.

    - **Локальная или доменная учетная запись**. Если выбран этот вариант, укажите учетную запись пользователя, от имени которой будет запускаться инсталлятор приложения. Нажмите на кнопку **Добавить**, выберите **Локальная или доменная 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 приложение 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 Linux поддерживает формат закрытых ключей PEM, а утилита ssh-keygen по умолчанию генерирует SSH-ключи в формате OPENSSH. Формат OPENSSH не поддерживается Kaspersky Security Center Linux. 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>"
      ```

11. Если на шаге мастера **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 в разделе **Задачи**.

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, выбранное приложение будет удалено на выбранных устройствах.

Ограничения удаленной деинсталляции

Иногда удаленная деинсталляция приложений сторонних производителей может завершится предупреждением: "Удаление на этом устройстве завершено с предупреждениями: Приложение для деинсталляции не установлено". Эта проблема возникает, когда приложение для деинсталляции, уже было деинсталлировано или было установлено только для одного пользователя. Приложения, установленные для одного пользователя (далее также "приложения для каждого пользователя"), становятся невидимыми и не могут быть деинсталлированы удаленно, если пользователь не вошел в систему.

Такое поведение отличается от поведения приложений, предназначенных для использования несколькими пользователями на одном устройстве (далее также "приложения устройства"). Приложения для каждого устройства видны и доступны всем пользователям этого устройства.

Поэтому приложения для каждого пользователя должны быть деинсталлированы только когда пользователь вошел в систему.

Источники информации об установленных приложениях

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 приложениях, установленных для всех пользователей.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о приложениях, установленных для всех пользователей.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о приложениях, установленных для текущего пользователя.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о приложениях, установленных для набора пользователей.

Подготовка устройства под управлением Windows к удаленной установке

Удаленная установка приложения на клиентском устройстве может завершаться с ошибкой по следующим причинам:

- Задача ранее уже была успешно выполнена на этом устройстве.

  В этом случае ее повторное выполнение не требуется.

- Во время запуска задачи устройство было выключено.

  В этом случае требуется включить устройство и запустить задачу еще раз.

- Отсутствует связь между Сервером администрирования и Агентом администрирования, установленным на клиентском устройстве.

  Для определения причины проблемы вы можете воспользоваться утилитой удаленной диагностики клиентского устройства (klactgui).

- Если на устройстве не установлен Агент администрирования, при удаленной установке приложения могут возникнуть следующие ситуации:

  - на клиентском устройстве включен параметр **Отключить простой общий доступ к файлам**;
  - на клиентском устройстве не работает служба Server;
  - на клиентском устройстве закрыты необходимые порты;
  - у учетной записи, под которой выполняется задача, недостаточно прав.

  Для того чтобы избежать проблем, которые могут возникнуть при установке приложения на клиентское устройство без установленного Агента администрирования, необходимо действовать, как описано в разделе принудительного развертывания с помощью задачи удаленной установки Kaspersky Security Center Linux.

Ранее использовалась утилита riprep для подготовки устройства к удаленной установке. Теперь это считается устаревшим способом настройки операционных систем. Утилиту riprep не рекомендуется использовать на операционных системах выше Windows XP и Windows Server 2003 R2.

Создание задачи Удаленное выполнение скриптов

Вы можете создать задачу *Удаленное выполнение скриптов* для выполнения инсталляционного пакета на клиентском устройстве и удаленной установки приложения.

Инсталляционный пакет содержит ZIP-архив с набором скриптов для выполнения на клиентских устройствах, а также файл manifest.json. Подробнее о создании этого типа инсталляционного пакета см. статью.

Эту задачу нужно запускать только на устройствах с Агентом администрирования для Linux.

Чтобы запустить задачу Удаленное выполнение скриптов:

1. Перейдите в **Мастер создания задачи** и выберите тип задачи **Удаленное выполнение скриптов**.
2. Введите название задачи и выберите устройства, которым будет назначена задача. Нажмите на кнопку **Далее**.
3. Выберите инсталляционный пакет на основе ZIP-архива с файлом manifest.json для удаленного выполнения.

   Если вы не хотите повторно запускать задачу на устройствах, на которых она уже была выполнена, включите параметр **Не запускать эту задачу на устройствах, на которых она уже была выполнена**.
4. Выберите учетную запись для запуска задачи.

   Если вы выберете учетную запись по умолчанию, то задачу будет выполнять Агент администрирования (учетная запись root).

   При запуске задачи *Удаленное выполнение скриптов* вы не можете изменить учетную запись, которая назначена задаче. Чтобы изменить учетную запись, которой назначена задача, остановите задачу в параметрах задачи и создайте задачу снова с требуемой учетной записью.
5. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
6. Нажмите на кнопку **Готово**.

   Задача *Удаленное выполнение скриптов* создана и отображается в списке задач.

После получения данных из задачи *Удаленное выполнение скриптов*, Агент администрирования ограничивает доступ к полученным данным для всех пользователей, кроме администратора и пользователя, указанного в параметрах задачи.

Создание инсталляционного пакета на основе манифест-файла

Чтобы создать инсталляционный пакета на основе манифест-файла:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Выберите параметр **Создать инсталляционный пакет для задачи "Удаленное выполнение скриптов" на основе архива ZIP с файлом manifest.json**.

4. Укажите имя инсталляционного пакета и нажмите на кнопку **Обзор**.

   В открывшемся окне выберите файл для создания инсталляционного пакета.

5. Выберите архивный файл, расположенный на доступных дисках. О том, как подготовить архив для этой задачи, см. статью.

   Файл начнет загружаться на Сервер администрирования Kaspersky Security Center Linux.

   Начнется процесс создания инсталляционного пакета.

   В окне мастера отобразится информация о завершении процесса.

   Если инсталляционный пакет не создан, отобразится соответствующее сообщение.

6. Нажмите на кнопку **Готово**, чтобы закрыть окно мастера.

Созданный инсталляционный пакет загружается во вложенную папку Packages общей папки Сервера администрирования. После загрузки инсталляционный пакет появится в списке инсталляционных пакетов.

В списке инсталляционных пакетов доступных на Сервере администрирования, нажав на имя инсталляционного пакета, вы можете:

- Просмотреть следующие свойства инсталляционного пакета:
  - **Имя.** Название инсталляционного пакета.
  - **Источник.** Имя поставщика приложения.
  - **Версия.** Версия приложения.
  - **Создано.** Дата создания инсталляционного пакета.
  - **Изменено.** Дата изменения инсталляционного пакета.
  - **Путь.** Путь к пользовательскому инсталляционному пакету на Сервере администрирования.
- Изменить имя пакета и параметры командной строки. Эта функция доступна только для пакетов, которые не созданы на основе приложений "Лаборатории Касперского".

Подготовка архива для задачи Удаленное выполнение скриптов

Архив для задачи *Удаленное выполнение скриптов* на основе файла manifest.json должен соответствовать следующим требованиям:

- Формат архива: ZIP.
- Общий размер: не более 1 ГБ.

- Количество файлов и папок в архиве не ограничено.
- Манифест-файл архива должен соответствовать приведенной ниже схеме и называться manifest.json. Схема проверяется только во время выполнения задачи на устройстве.

  Схема JSON манифест-файла и описание массивов

  Схема JSON

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
                    },
                    "path": {
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
                    "results":{
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
                                },
                                "next":{
                                    "type": "string",
                                    "enum": ["break", "continue"]
                                }
                            },
                            "required": [
                                "code",
                                "next"
                            ]
                        }
                    },
```

```
                    "default_next":{
                        "type": "string",
                        "enum": ["break", "continue"]
                    }
                },
                "required": [
                    "type",
                    "path",
                    "default_next"
                ]
            }
        }
    },
    "required": [
        "version",
        "actions"
    ]
}
```

Пример манифест-файла

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
```

```
  ]
}
```

- Архив должен иметь следующую структуру:

```
manifest.json
<file1>
<file2>
<folder1>/<file3>
<folder2>/<folder3>/<file4>
...
<fileX>
```

`manifest.json` – это манифест-файл задачи.

`<file1>`, ..., `<fileX>` – это набор файлов со скриптами, которые нужно выполнить.

Удаленная установка приложений на устройства с помощью задачи Удаленное выполнение скриптов

Задачу *Удаленное выполнение скриптов* можно использовать для удаленной установки приложения на клиентское устройство с помощью создания пользовательского инсталляционного пакета.

О том, как подготовить архив для этой задачи, см. статью.

Чтобы создать инсталляционный пакет для удаленной установки приложения на клиентское устройство, в архив, который вы хотите загрузить для этой задачи, должны быть включены следующие файлы:

- `<имя пакета>.deb`
- **install.sh**

  ```
  sudo apt-get install <имя пакета>.deb
  ```

- **manifest.json**

  Схема JSON для удаленной установки приложения

  ```
  {
    "version": 1,
    "actions": [
      {
        "type": "execute",
        "path": "install.sh",
        "args": "<введите аргументы, если необходимо>",
        "results": [
          {
            "code": 0,
            "next": "continue"
          }
        ],
        "default_next": "break"
      }
  ```

```
  ]
}
```

Описание массивов

1. `version` – версия файла манифеста и задачи.

   В настоящее время единственное допустимое значение – 1.

2. Элементы массива `actions` определяют состав и порядок выполнения скриптов в задаче.

   Порядок выполнения скрипта соответствует индексу (положению) элемента в массиве.

3. Для каждого элемента массива `actions` определены следующие элементы.

   a. `type` – тип исполняемой команды из скриптов. В настоящее время значение всегда `execute`.

   b. `path` – путь к файлу скрипта в архиве.

   c. `args` – аргументы, которые передаются скрипту как часть исполняемой команды.

   d. `results` – массив, определяющий дальнейшие действия в зависимости от результата выполнения задачи.

      1. `code` – значение, возвращающее скрипт.

      2. `next` – действие, которое будет выполнено следующим. Действие `continue` переходит к выполнению следующего скрипта (элемента в массиве `actions`). Действие `break` останавливает задачу.

   e. `default_next` – действие, если скрипт возвращает значение, которого нет в `results`.

При запуске задачи *Удаленное выполнение скриптов* Агент администрирования загрузит инсталляционный пакет с приложением на клиентское устройство. Когда клиентское устройство получает инсталляционный пакет, Агент администрирования на этом устройстве анализирует файл manifest.json и определяет порядок выполнения скриптов и действий в зависимости от результата, а затем начинает выполнение.

После завершения задачи *Удаленное выполнение скриптов* приложение будет установлено на клиентском устройстве.

Настройка уведомлений и мониторинга для задачи Удаленное выполнение скриптов

Вы можете настроить мониторинг, поведение при сохранении событий и уведомления для задачи *Удаленное выполнение скриптов*.

Чтобы просмотреть статус задачи Удаленное выполнение скриптов:

1. В главном окне приложения перейдите в раздел **Задачи**.

   Отобразится список задач.

2. Выберите задачу и нажмите на **История устройства**.

   Отображается ход выполнения задачи.

Чтобы настроить поведение при сохранении событий:

1. В списке задач нажмите на название задачи и перейдите на вкладку **Параметры**.
2. В разделе **Уведомления** нажмите на кнопку **Параметры**.
3. Выберите один из следующих вариантов поведения приложения после выполнения задачи:

   - **Сохранять все события**.
   - **Сохранять события, связанные с ходом выполнения задачи**.
   - **Сохранять только результат выполнения задачи**.

     События сохраняются в разделе **История устройства** и **Хранилище событий**.

     По умолчанию сохраняются только результаты выполнения задачи.

     > Если вы выберете **Сохранять все события**, сохраняются только результаты выполнения задачи.

4. Если вы хотите сохранить события в базе данных Сервера администрирования, в журнале событий на Сервере администрирования или на устройстве, включите соответствующий параметр.

Подробнее о настройке уведомлений см. в этой статье.

Лицензирование

Этот раздел содержит информацию:

- Общие понятия, связанные с лицензированием Kaspersky Security Center Linux.
- Инструкция по управлению лицензиями управляемых приложений "Лаборатории Касперского".

Лицензирование Kaspersky Security Center Linux

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием Kaspersky Security Center Linux.

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского" в котором указано, на каких условиях вы можете использовать приложение.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с приложением.

Kaspersky Security Center 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;
- 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 приложения. Если вы не согласны с условиями Лицензионного соглашения, вам нужно прервать установку приложения и не должны использовать приложение.

О лицензии

Лицензия – это ограниченное по времени право на использование Kaspersky Security Center, предоставляемое вам на условиях заключенного Лицензионного договора (Лицензионного соглашения).

Список доступных функций и срок использования приложения зависят от лицензии, по которой используется приложение.

Предусмотрены следующие типы лицензий:

- *Пробная*

  Бесплатная лицензия, предназначенная для ознакомления с приложением. Пробная лицензия имеет небольшой срок действия.

  По истечении срока действия пробной лицензии Kaspersky Security Center Linux прекращает выполнять все свои функции. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.

  Вы можете использовать приложение по пробной лицензии только в течение одного срока пробного использования.

- *Коммерческая*

  Платная лицензия.

  По истечении срока действия коммерческой лицензии приложение прекращает выполнять свои основные функции. Для продолжения работы Kaspersky Security Center вам нужно продлить срок действия коммерческой лицензии. После истечения срока действия лицензии вы не можете далее использовать приложение и должны удалить его с устройства.

  Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить непрерывность защиты устройства 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:

- идентификатор лицензии или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о приложении, которое можно активировать по предоставляемой лицензии;

- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать приложение по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О лицензионном ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать приложение в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить лицензионный ключ в приложение одним из следующих способов: применить *файл ключа* или ввести *код активации*. Лицензионный ключ отображается в интерфейсе приложения в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в приложение.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы приложения требуется добавить другой лицензионный ключ.

Лицензионный ключ может быть активным и дополнительным (или резервным).

Активный лицензионный ключ – лицензионный ключ, используемый в текущий момент для работы приложения. В качестве активного может быть добавлен лицензионный ключ для пробной или коммерческой лицензии. В приложении не может быть больше одного активного лицензионного ключа.

Дополнительный (или резервный) лицензионный ключ – лицензионный ключ, подтверждающий право на использование приложения, но не используемый в текущий момент. Дополнительный лицензионный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным лицензионным ключом. Дополнительный лицензионный ключ может быть добавлен только при наличии активного лицензионного ключа.

Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии не может быть добавлен в качестве дополнительного лицензионного ключа.

Просмотр Политики конфиденциальности

Политика конфиденциальности доступна в интернете на странице https://www.kaspersky.ru/products-and-services-privacy-policy.

Политика конфиденциальности также доступна в автономном режиме:

- Вы можете ознакомиться с Политикой конфиденциальности перед установкой Kaspersky Security Center Linux.
- Текст Политики конфиденциальности находится в файле license.txt в папке установки Kaspersky Security Center Linux.

- Файл privacy_policy.txt доступен на управляемом устройстве в папке Агента администрирования.
- Вы можете распаковать файл privacy_policy.txt из дистрибутива Агента администрирования.

Варианты лицензирования Kaspersky Security Center

Kaspersky Security Center может работать в следующих режимах:

- **Базовая функциональность Консоли администрирования**

  Kaspersky Security Center работает в этом режиме до активации приложения или после истечения срока действия коммерческой лицензии. Приложение Kaspersky Security Center с поддержкой базовой функциональности Консоли администрирования поставляется в составе приложений "Лаборатории Касперского", предназначенных для защиты сети организации. Кроме того, она доступна для загрузки с веб-сайта "Лаборатории Касперского".

- **Коммерческая лицензия**

  Если вам нужна дополнительная функциональность, не входящая в базовую функциональность Консоли администрирования, вам требуется приобрести коммерческую лицензию.

  При добавлении лицензионного ключа в окне свойств Сервера администрирования убедитесь, что вы добавили лицензионный ключ, который позволяет использовать Kaspersky Security Center Linux. Вы можете найти эту информацию на сайте "Лаборатории Касперского". На странице каждого решения есть список приложений, включенных в это решение. Сервер администрирования может принимать неподдерживаемые лицензионные ключи, например лицензионный ключ для Kaspersky Endpoint Security Cloud, но такие лицензионные ключи не предоставляют никаких новых функций, кроме базовой функциональности Консоли администрирования.

Функция или свойство	Режим работы приложения Kaspersky Security Center Linux	
	Лицензия отсутствует	Коммерческая лицензия
Базовая функциональность Консоли администрирования Доступны следующие функции: • создание виртуальных Серверов администрирования для управления сетью удаленных офисов или организаций-клиентов; • формирование иерархии групп администрирования для управления набором устройств как единым целым; • удаленная установка приложений; • централизованная настройка параметров приложений, установленных на клиентских устройствах; • контроль состояния антивирусной безопасности организации; • управление ролями пользователей; • получение статистики и отчетов о работе приложений, а также уведомлений о критических событиях; • централизованная работа с файлами, помещенными на карантин или в резервное хранилище, а также с файлами, обработка которых отложена; • управление процессом шифрования и защиты данных; • просмотр и редактирование вручную списка оборудования, обнаруженного в результате опроса сети; • просмотр списка образов операционных систем, доступных для удаленной установки.	✓	✓

Функция или свойство	Режим работы приложения Kaspersky Security Center Linux	
	Лицензия отсутствует	Коммерческая лицензия
Системное администрирование: базовая функциональность Для следующих задач не требуется коммерческая лицензия: • Задача *Поиск уязвимостей и требуемых обновлений*. С помощью этой задачи Kaspersky Security Center Linux получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, установленных на управляемых устройствах. • Задача *Закрытие уязвимостей* Задача *Закрытие уязвимостей* использует рекомендованные исправления приложений Microsoft и пользовательские исправления для приложений сторонних производителей. Чтобы использовать эту задачу, требуется вручную указать пользовательские исправления для закрытия уязвимостей, которые указаны в параметрах задачи.	✓	✓
Системное администрирование: расширенная функциональность Вы можете определить правила автоматической удаленной установки обновлений программного обеспечения и автоматического закрытия уязвимостей.	—	✓
Управление системами Доступны следующие функции: • удаленное разрешение подключения к клиентским устройствам с помощью компонента Microsoft Windows "Подключение к удаленному рабочему столу"; • удаленное подключение к клиентским устройствам с помощью совместного доступа к рабочему столу Windows.	—	✓
Экспорт событий в SIEM-системы с помощью формата Syslog По протоколу Syslog можно передавать любые события, произошедшие на Сервере администрирования Kaspersky Security Center и в приложениях "Лаборатории Касперского", установленных на управляемых устройствах. Протокол Syslog – это стандартный протокол регистрации сообщений. Вы можете использовать этот протокол для экспорта событий в любую SIEM-систему.	✓	✓
Агрегирование алертов и выполнение действий по реагированию с помощью Active Directory, KASAP и Kaspersky TIP Sandbox.	—	✓

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего приложение.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Security Center или после заказа пробной версии Kaspersky Security Center.

Чтобы активировать приложение с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- Обратиться к продавцу лицензии.
- Получить файл ключа на веб-сайте "Лаборатории Касперского" на основе имеющегося кода активации.

О предоставлении данных

Данные, передаваемые третьим сторонам

При использовании Программным обеспечением функциональности для Управления мобильными устройствами для своевременной доставки команд на устройства под управлением операционной системы Android через механизм push-уведомлений используется сервис Google Firebase Cloud Messaging. Если Пользователь настроил использование сервиса Google Firebase Cloud Messaging, Пользователь соглашается предоставлять следующую информацию сервису Google Firebase Cloud Messaging в автоматическом режиме:

- Идентификатор экземпляра.
- Идентификатор программного обеспечения в службе Google Firebase Cloud Messaging.
- Версия установленного программного обеспечения.
- Полная версия программного обеспечения.
- Версия Google Play.
- Название дистрибутива программного обеспечения.
- Версия схемы для предоставляемых данных.
- Версия операционной системы.
- Идентификатор программного обеспечения.

Чтобы блокировать обмен информацией со службой Google Firebase Cloud Messaging, Пользователь должен сбросить настройки использования службы Google Firebase Cloud Messaging.

При использовании Программным обеспечением функциональности для Управления мобильными устройствами для своевременной доставки команд на устройства под управлением операционной системы iOS через механизм push-уведомлений используется сервис Apple Push Notification Service (APNs). Если Пользователь установил APNs-сертификат на сервер iOS MDM, сформировал iOS MDM-профиль с набором параметров подключения мобильных устройств iOS к Программному обеспечению и установил этот iOS MDM-профиль на мобильные устройства, Пользователь соглашается в автоматическом режиме предоставлять в сервис APNs следующую информацию:

- Токен – push-токен устройства. Сервер использует этот токен при отправке push-уведомлений на устройство.
- PushMagic – строка, которая должна быть включена в push-уведомление. Значение строки генерируется устройством.

Данные, передаваемые в АО "Лаборатория Касперского"

Если Пользователю доступна функциональность Kaspersky Extended Detection and Response Optimum, Kaspersky Security Center Linux передает данные в следующих случаях:

- Для назначения сотруднику курса обучения Kaspersky Security Center Linux передает в Kaspersky Automated Security Awareness Platform (KASAP) следующие данные: адрес электронной почты пользователя, дополнительный адрес электронной почты пользователя (при наличии), идентификатор пользователя в KASAP, идентификатор группы обучения.

- Для автоматического запуска файла с помощью Kaspersky Cloud Sandbox, управляемое приложение передает файлы, помещенные в Карантин, с Сервера администрирования с помощью Агента администрирования, а затем с помощью Kaspersky Security Center Web Console в Kaspersky Cloud Sandbox. Kaspersky Cloud Sandbox выполняет анализ переданного файла и файлов, которые могут быть созданы в ходе выполнения переданного файла.

Данные, обрабатываемые локально

Приложение Kaspersky Security Center Linux предназначено 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 приложений "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 приложений "Лаборатории Касперского" на устройства;

- управление параметрами работы и задачами установленных приложений;

- управление обновлениями приложений "Лаборатории Касперского" и других производителей, поиск и закрытие уязвимостей;

- активация приложений "Лаборатории Касперского" на устройствах;

- управление учетными записями пользователей;

- просмотр информации о работе приложений "Лаборатории Касперского" на устройствах;

- просмотр отчетов;

- включение интеграции со службами "Лаборатории Касперского".

Для выполнения своих основных функций приложение Kaspersky Security Center Linux может принимать, хранить и обрабатывать следующую информацию:

- Информацию об устройствах в сети организации, полученную с помощью опроса контроллеров домена (Active Directory, Samba, FreeIPA и ALD Pro) или с помощью опроса IP-диапазонов. Сервер администрирования самостоятельно получает данные или передает Агенту администрирования.

- Информацию от контроллеров домена (Active Directory, Samba, FreeIPA и ALD Pro) о подразделениях, доменах, пользователях и группах. Сервер администрирования самостоятельно получает данные, или их передает ему Агент администрирования, который выполняет роль точки распространения.

- Данные об управляемых устройствах. Агент администрирования передает от устройства Серверу администрирования перечисленные ниже данные. Пользователь вводит отображаемое имя и описание устройства в интерфейсе Kaspersky Security Center Web Console:

  - Технические характеристики управляемого устройства и его компонентов, необходимые для идентификации устройства: отображаемое имя и описание устройства, имя и тип Windows-домена (для устройств, принадлежащих Windows-домену), имя устройства в среде Windows (для устройств, принадлежащих Windows-домену), DNS-домен и DNS-имя, IPv4-адрес, IPv6-адрес, сетевое местоположение, MAC-адрес, серийный номер, тип операционной системы, является ли устройство виртуальной машиной и тип гипервизора, а также является ли устройство динамической виртуальной машиной в составе VDI.

  - Прочие характеристики управляемых устройств и их компонентов, необходимые для аудита управляемых устройств и для принятия решений о применимости тех или иных патчей и обновлений: архитектура операционной системы, поставщик операционной системы, номер сборки операционной системы, идентификатор выпуска операционной системы, папка расположения операционной системы, если устройство является виртуальной машиной, то тип виртуальной машины, имя виртуального Сервера администрирования, под управлением которого находится устройство.

  - Подробные данные о действиях на управляемых устройствах: дата и время последнего обновления, время, когда устройство последний раз было видимо в сети, состояние ожидания перезапуска, время включения устройства.

  - Данные об учетных записях пользователей устройств и их сеансах работы.

- Данные, полученные при запуске удаленной диагностики на управляемом устройстве: файлы трассировки, системная информация, сведения об установленных на устройстве приложениях "Лаборатории Касперского", файлы дампов, журналы событий, результаты запуска диагностических скриптов, полученные от Службы технической поддержки "Лаборатории Касперского".

- Статистику работы точки распространения, если устройство является точкой распространения. Агент администрирования передает данные от устройства на Сервер администрирования.

- Параметры точки распространения, которые Пользователь вводит в Kaspersky Security Center Web Console.

- Данные, необходимые для подключения мобильных устройств к Серверу администрирования: сертификат, порт для подключения мобильных устройств, адрес подключения к Серверу администрирования. Пользователь вводит данные в Kaspersky Security Center Web Console.

- Данные о мобильных устройствах, передаваемые по протоколу мобильной связи. Данные перечисленные ниже передаются от мобильного устройства Серверу администрирования:
    - Информация о приложении: название приложения, полная версия приложения, дата и время установки приложения, статус постоянной защиты устройства, идентификатор сеанса.
    - Информация о лицензионных ключах, используемых приложением: серийный номер лицензионного ключа и тип лицензионного ключа, статус лицензионного ключа, срок годности лицензионного ключа в днях, даты вступления в действие и дата истечения срока действия лицензии, название компании, которой была предоставлена лицензия, дополнительная информация в случае использования подписки (флаг подписки, дата истечения срока действия и количество дней, доступных для продления подписки, веб-адрес поставщика подписки, текущий статус подписки и причина получения этого статуса), дата и время активации приложения на устройстве, дата и время истечения срока действия лицензии на устройстве.
    - Информация об управляемом устройстве: название устройства, идентификатор устройства, тип устройства, IMEI устройства (если доступно), серийный номер устройства (если доступно), производитель устройства, название семейства процессоров устройства, отпечаток сертификата владельца устройства, тип операционной системы, версия операционной системы, название операционной системы, общий объем дискового пространства на устройстве, название сервера, к которому принадлежит устройство, IP-адрес устройства, название группы устройства, отличительное имя пользователя, отличительное имя домена, одноразовый пароль или доменный пароль.
    - Информация о результатах выполнения пользовательских команд: идентификатор команды, статус выполнения команды, результат выполнения команды; для команды определения местоположения устройства: широта, долгота, высота и скорость движения устройства; для команды выполнения фотографии: фотографии, сделанные фронтальной камерой мобильного устройства при попытке разблокировать устройство.
    - Информация о проверке устройства: дата и время последней проверки устройства; полный путь в файловой системе, с которого началась проверка; количество проверенных объектов; количество обнаруженных вредоносных объектов; количество заблокированных, удаленных и вылеченных объектов; количество объектов, которые не удалось вылечить; количество ошибок валидации; количество завершенных процессов.
    - Информация о функционировании каждого компонента приложения и о выполнении каждой задачи, представленная в виде событий:
        - Идентификатор события.
        - Уровень важности.
        - Название и тип события.
        - Описание причины события.
        - Дата и время возникновения события.
        - Информация о событиях операции Анти-Вор (код разблокировки устройства, координаты устройства, метод доставки команды, список удаленных данных).
        - Результаты обработки обнаруженного объекта или действия (имя файла на устройстве; название приложения; название угрозы; тип угрозы; тип выполненного действия с файлом; результат действия; код ошибки, в случае ее появления).
        - Информация о сработавшем правиле соответствия (критерий правила; примененное действие; описание ошибки при применении действия, в случае ее возникновения).

- Информация об ошибке работы приложения (версия приложения, версия ОС, название устройства, описание ошибки).
- Информация об ошибке Samsung KNOX (код ошибки, URL, с которого не удалось загрузить файл).
- Информация о разрешениях, предоставленных приложению.
- Информация о каждом из приложений, установленных на управляемом устройстве (название приложения, статус установки).
- Информация о глобальном принятии Лицензионного соглашения: идентификатор Лицензионного соглашения, временная метка Лицензионного соглашения, текст Лицензионного соглашения.
- Параметры Google Firebase Cloud Messaging: Sender ID, идентификатор регистрации устройства.

- Информация о публичном IP-адресе устройства.
- Значения пользовательских параметров. Администратор настраивает параметры в Kaspersky Security Center Web Console, пользователь задает значения этих параметров через мобильное приложение.

- Данные о мобильных устройствах, передаваемые по протоколу iOS MDM. Данные перечисленные ниже передаются от мобильного устройства Серверу администрирования:
  - Технические характеристики мобильного устройства и его компонентов, необходимые для идентификации устройства: имя устройства, модель, название операционной системы, версия и номер сборки, номер модели устройства, номер IMEI, номер телефона, UDID, MEID, серийный номер, объем полной и доступной памяти, версия прошивки модема, MAC-адрес Bluetooth, MAC-адрес Wi-Fi и данные SIM-карты (код ICCID как часть идентификатора SIM-карты).
  - Данные о мобильной сети, используемой мобильным устройством: тип мобильной сети, название используемой мобильной сети, название домашней мобильной сети, версия параметров оператора мобильной сети, статус голосового роуминга и роуминга данных, код страны для домашней сети, код страны пребывания, код страны используемой сети и уровень шифрования.
  - Параметры безопасности мобильного устройства: использование пароля и его соответствие параметрам политики, список установленных сертификатов, список приложений и конфигурационных профилей.
  - Дата и время последней синхронизации с Сервером администрирования и статус управления устройством.
- Подробная информация о данных мобильного устройства, передаваемых по протоколу WebRTC: снимок экрана устройства.
- Дополнительные сведения о файлах, указанных для передачи на мобильные устройства. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.

- Данные о приложениях "Лаборатории Касперского", установленных на устройстве. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования:

  - Параметры приложений "Лаборатории Касперского", установленных на управляемом устройстве: название и версия приложения "Лаборатории Касперского", статус, состояние постоянной защиты, дата и время последней проверки устройства, количество обнаруженных угроз, количество объектов, для которых не удалось выполнить лечение, наличие и статус компонентов приложения, данные о параметрах и задачах приложения "Лаборатории Касперского", информация об активном и резервных лицензионных ключах, дата и идентификатор установки приложения.

  - Статистика работы приложения: события, связанные с изменениями статуса компонентов приложения "Лаборатории Касперского" на управляемом устройстве и с выполнением задач, инициированных компонентами приложения.

  - Состояние устройства, определенное приложением "Лаборатории Касперского".

  - Теги, передаваемые приложением "Лаборатории Касперского".

- Данные, содержащиеся в событиях от компонентов Kaspersky Security Center Linux и управляемых приложений "Лаборатории Касперского". Агент администрирования передает данные от устройства на Сервер администрирования.

- Данные, необходимые для интеграции Kaspersky Security Center Linux с SIEM-системой для экспорта событий. Пользователь вводит данные в Kaspersky Security Center Web Console.

- Данные, необходимые для интеграции Kaspersky Security Center Linux с контроллерами домена (Active Directory, Samba, FreeIPA и ALD Pro). Пользователь вводит данные в Kaspersky Security Center Web Console.

- Файлы keytab для подключения с Kerberos Single Sign-On (SSO). Пользователь вводит данные в Kaspersky Security Center Web Console.

- Данные, необходимые для настройки подключения к прокси-серверу для подключения к интернету. Пользователь вводит данные в Kaspersky Security Center Web Console.

- Настройки компонентов Kaspersky Security Center Linux и управляемых приложений "Лаборатории Касперского", представленные в виде политик и профилей политик. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.

- Настройки задач компонентов Kaspersky Security Center Linux и управляемых приложений "Лаборатории Касперского". Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.

- Данные, обрабатываемые функцией Системное администрирование. Агент администрирования передает с устройства на Сервер администрирования следующую информацию:

  - Информация об оборудовании, обнаруженном на управляемых устройствах (Реестр оборудования).

    Если Агент администрирования установлен на устройстве с операционной системой Windows, он отправляет на Сервер администрирования следующую информацию об аппаратном обеспечении устройства:

    - оперативная память;

    - запоминающие устройства;

    - материнская плата;

- процессор;
- сетевой адаптер;
- мониторы;
- видеоадаптер;
- звуковая плата.

Если Агент администрирования установлен на устройстве с операционной системой Linux или macOS, он отправляет на Сервер администрирования следующую информацию об аппаратном обеспечении устройства, если эта информация предоставляется операционной системой:

- общий объем оперативной памяти;
- общий объем запоминающих устройств;
- материнская плата;
- процессор;
- сетевой адаптер.

- Данные о приложениях и патчах, установленных на управляемых устройствах (Реестр приложений). Приложения могут быть сопоставлены с информацией об исполняемых файлах, обнаруженных на управляемых устройствах функцией Контроль приложений.
- Данные об уязвимостях стороннего программного обеспечения, обнаруженных на управляемых устройствах.
- Данные об обновлениях, доступных для сторонних приложений, установленных на управляемых устройствах.

- Данные, которые необходимы для загрузки обновлений на изолированный Сервер администрирования для закрытия уязвимостей в приложениях сторонних производителей на управляемых устройствах. Пользователь вводит и передает данные с помощью утилиты klscflag Сервера администрирования.
- Пользовательские категории приложений. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Данные об исполняемых файлах, обнаруженных на управляемых устройствах функцией Контроль приложений. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Данные о файлах, помещенных в резервное хранилище. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Данные о файлах, помещенных в Карантин. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Данные о файлах, запрошенных специалистами "Лаборатории Касперского" для подробного анализа. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Данные о состоянии и срабатывании правил Адаптивного контроля аномалий. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Данные о внешних устройствах (устройствах памяти, инструментах передачи информации, инструментах превращения информации в твердую копию, шинах подключения), установленных или подключенных к управляемому устройству и обнаруженных функцией Контроль устройств. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Информация о зашифрованных устройствах на базе Windows и статусе шифрования. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования.

- Информация об ошибках шифрования данных на устройствах. Шифрование выполняется функцией Шифрование данных приложений "Лаборатории Касперского". Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Список управляемых программируемых логических контроллеров (ПЛК). Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Данные для создания цепочки развития угроз. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Информация о попытках сотрудников организации получить доступ к облачным сервисам. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Данные, необходимые для интеграции Kaspersky Security Center со службой Kaspersky Managed Detection and Response (для Kaspersky Security Center Web Console должен быть установлен специальный плагин): токен инициации интеграции, токен интеграции и токен сеанса пользователя. Пользователь с помощью токена инициации интеграции входит в интерфейс Kaspersky Security Center Web Console. Служба Kaspersky MDR передает токен интеграции и токен сеанса пользователя через специальный плагин.

- Данные, необходимые для интеграции Kaspersky Security Center Linux с Kaspersky Cloud Sandbox и Kaspersky Threat Intelligence Portal (требуется установка соответствующего плагина для Kaspersky Security Center Web Console): токен интеграции, токен авторизации. Пользователь вводит токен для интеграции в интерфейсе Kaspersky Security Center Web Console. Kaspersky Security Center Web Console передает токен для авторизации в запросе к Kaspersky Cloud Sandbox API.

- Данные, необходимые для интеграции Kaspersky Security Center Linux со службой Kaspersky Automated Security Awareness Platform (KASAP): API-токен для доступа к KASAP OpenAPI, URL (ссылка для доступа к KASAP через OpenAPI).

- Данные о введенных кодах активации и файлах ключей. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.

- Учетные записи пользователей: имя, описание, полное имя, адрес электронной почты, основной номер телефона, пароль, секретный ключ, сгенерированный Сервером администрирования, и одноразовый пароль для двухфакторной аутентификации. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.

- Истории ревизий объектов управления. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.

- IP-адрес устройства, на котором пользователь создал ревизию. IP-адрес определяется Сервером администрирования автоматически.
- Реестр удаленных объектов управления. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Инсталляционные пакеты, созданные из файла, и параметры установки. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Данные, необходимые для отображения объявлений от "Лаборатории Касперского" в Kaspersky Security Center Web Console. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Данные, необходимые для работы плагинов управляемых приложений в Kaspersky Security Center Web Console и сохраняемые плагинами в базе данных Сервера администрирования в процессе повседневной работы. Описание и способы предоставления данных приведены в файлах справки соответствующего приложения.
- Настройки пользователя Kaspersky Security Center Web Console: язык локализации и тема пользовательского интерфейса, настройки отображения панели мониторинга, информации о состоянии нотификаций (прочитано/не прочитано), состояние столбцов в таблицах (скрыть/показать), прогресс прохождения режима обучения. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Сертификат безопасного подключения управляемых устройств к компонентам Kaspersky Security Center Linux. Пользователь вводит и передает данные с помощью утилиты klsetsrvcert Сервера администрирования.
- Сертификаты для установки доверия к внутренним веб-ресурсам организации. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Информация о принятии пользователем условий юридических соглашений с "Лабораторией Касперского".
- Данные Сервера администрирования, которые Пользователь вводит в интерфейсе Kaspersky Security Center Web Console или в программном интерфейсе Kaspersky Security Center OpenAPI.
- Любые данные, которые Пользователь вводит в интерфейсе Kaspersky Security Center Web Console.

Перечисленные выше данные могут попасть в Kaspersky Security Center Linux следующими способами:

- Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Агент администрирования самостоятельно получает данные с устройства и передает на Сервер администрирования.
- Агент администрирования получает данные от управляемого приложения "Лаборатории Касперского" и передает их на Сервер администрирования. Перечни данных, обрабатываемых управляемыми приложениями "Лаборатории Касперского", приведены в справках соответствующих приложений.
- Сервер администрирования самостоятельно получает данные о сетевых устройствах, или их передает ему Агент администрирования, который выполняет роль точки распространения.
- Данные передаются с мобильного устройства на Сервер администрирования по протоколу iOS MDM или по протоколу мобильной связи.

Перечисленные данные хранятся в базе данных Сервера администрирования. Хеши паролей 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.

Файлы дампов, файлы трассировки или файлы журналов компонентов Kaspersky Security Center Linux содержат произвольные данные Сервера администрирования, Агента администрирования и Kaspersky Security Center Web Console. Эти файлы могут содержать персональные или прочие конфиденциальные данные. Файлы дампов, файлы трассировки или файлы журналов хранятся на устройствах в незашифрованной форме. Файлы дампов, файлы трассировки или файлы журналов не передаются в "Лабораторию Касперского" автоматически, однако, администратор может передать эти файлы в "Лаборатории Касперского" вручную по запросу Службы технической поддержки для решения проблем в работе Kaspersky Security Center Linux.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

Переходя по ссылкам в Kaspersky Security Center Web Console, Пользователь соглашается на автоматическую передачу следующих данных:

- код Kaspersky Security Center Linux;
- версия Kaspersky Security Center Linux;
- язык локализации 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 приложения 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 приложения 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 приложения сохраняется.

Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky Security Center.

При использовании приложения по подписке Kaspersky Security Center Linux автоматически обращается к серверу активации через определенные промежутки времени вплоть до даты окончания подписки. Если доступ к серверу через системный DNS невозможен, приложение использует публичные DNS-серверы. Вы можете продлить подписку на веб-сайте поставщика услуг.

Активация Kaspersky Security Center Linux

Вы можете активировать Kaspersky Security Center Linux, чтобы использовать его дополнительные функции. Эту задачу можно выполнить двумя способами: с помощью мастера первоначальной настройки Сервера администрирования или с помощью настройки параметров Сервера администрирования.

Чтобы активировать Kaspersky Security Center Linux:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Лицензионные ключи**.

3. В разделе **Действующая лицензия** нажмите на кнопку **Выбрать**.

4. В открывшемся окне выберите лицензионный ключ, который вы хотите использовать для активации Kaspersky Security Center Linux. Если лицензионного ключа нет в списке, нажмите на кнопку **Добавить лицензионный ключ** и укажите новый лицензионный ключ.

5. При необходимости вы также можете добавить резервный лицензионный ключ. Для этого в разделе **Резервный лицензионный ключ** нажмите на кнопку **Выбрать** и выберите существующий лицензионный ключ или добавьте ключ. Обратите внимание, что вы не можете добавить резервный лицензионный ключ, если нет активного лицензионного ключа.

6. Нажмите на кнопку **Сохранить**.

Лицензирование управляемых приложений "Лаборатории Касперского"

В этом разделе описаны возможности Kaspersky Security Center по работе с лицензионными ключами управляемых приложений "Лаборатории Касперского".

Kaspersky Security Center Linux позволяет централизованно распространять лицензионные ключи приложений "Лаборатории Касперского" на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.

При добавлении лицензионного ключа с помощью Kaspersky Security Center свойства лицензионного ключа сохраняются на Сервере администрирования. На основании этой информации приложение формирует отчет об использовании лицензионных ключей и уведомляет администратора об истечении сроков действия лицензий и о превышении лицензионных ограничений, заложенных в свойствах лицензионных ключей. Вы можете настраивать параметры оповещений об использовании лицензионных ключей в составе параметров Сервера администрирования.

Лицензирование управляемых приложений

Приложения "Лаборатории Касперского" установленные на управляемых устройствах, должны быть активированы путем применения файла ключа или кода активации к каждому из приложений. Файл ключа или код активации может быть распространен следующими способами:

- с помощью автоматического распространения;
- с помощью инсталляционного пакета управляемого приложения;
- с помощью задачи добавления лицензионного ключа управляемого приложения;
- активация управляемого приложения вручную.

Вы можете добавить активный или резервный лицензионный ключ любым из перечисленных выше способов. Приложение "Лаборатории Касперского" использует активный в данный момент ключ и сохраняет резервный ключ, который будет применяться после истечения срока действия активного ключа. Приложение, для которого вы добавляете лицензионный ключ, определяет, является ли ключ активным или резервным. Определение ключа не зависит от способа, который вы используете для добавления лицензионного ключа.

Автоматическое распространение

Если вы используете разные управляемые приложения и вам важно распространить определенный файл ключа или код активации на устройства, используйте другие способы распространения кода активации или файла ключа.

Kaspersky Security Center позволяет автоматически распространять имеющиеся лицензионные ключи на устройства. Например, в хранилище Сервера администрирования находится три лицензионных ключа. Вам нужно включить параметр **Автоматически распространяемый лицензионный ключ** для всех трех лицензионных ключей. На устройствах организации установлено приложение безопасности "Лаборатории Касперского", например, Kaspersky Endpoint Security для Linux. Обнаружено новое устройство, на которое необходимо распространить лицензионный ключ. Приложение определяет, что для этого устройства подходит, например, два лицензионных ключа из хранилища, лицензионный ключ *Ключ_1* и лицензионный ключ *Ключ_2*. На устройство распространяется один из подходящих лицензионных ключей. В этом случае невозможно предсказать, какой из этих двух лицензионных ключей будет распространен на данное устройство, так как автоматическое распространение лицензионных ключей не предполагает вмешательства администратора.

При распространении лицензионного ключа на устройства происходит подсчет устройств для данного лицензионного ключа. Вам необходимо удостовериться, что количество устройств, на которые распространяется лицензионный ключ, не превышает лицензионное ограничение. В случае если количество устройств превышает лицензионное ограничение, 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 приложения.
- Виртуальный Сервер администрирования не имеет управляемых устройств.
- Лицензионный ключ уже используется для устройств, управляемых другим виртуальным Сервером администрирования, и достигнуто лицензионное ограничение на количество устройств.

Добавление файла ключа или кода активации в инсталляционный пакет управляемого приложения

Из соображений безопасности не рекомендуется использовать этот параметр. Файл ключа или код активации, добавленный в инсталляционный пакет, может быть скомпрометирован.

В случае установки управляемого приложения с помощью инсталляционного пакета вы можете указать код активации или файл ключа в инсталляционном пакете или в политике этого приложения. Лицензионный ключ распространится на управляемые устройства при очередной синхронизации устройства с Сервером администрирования.

Инструкция: Добавление лицензионного ключа в инсталляционный пакет

Распространение с помощью задачи добавления лицензионного ключа управляемого приложения

В случае использования задачи добавления лицензионного ключа управляемого приложения вы можете выбрать лицензионный ключ, который необходимо распространить на устройства, и выбрать устройства удобным вам способом, например, выбрав группу администрирования или выборку устройств.

Перед распространением файл ключа или код активации необходимо добавить в хранилище Сервера администрирования.

Инструкции:

- Добавление лицензионного ключа в хранилище Сервера администрирования.
- Распространение лицензионного ключа на клиентские устройства.

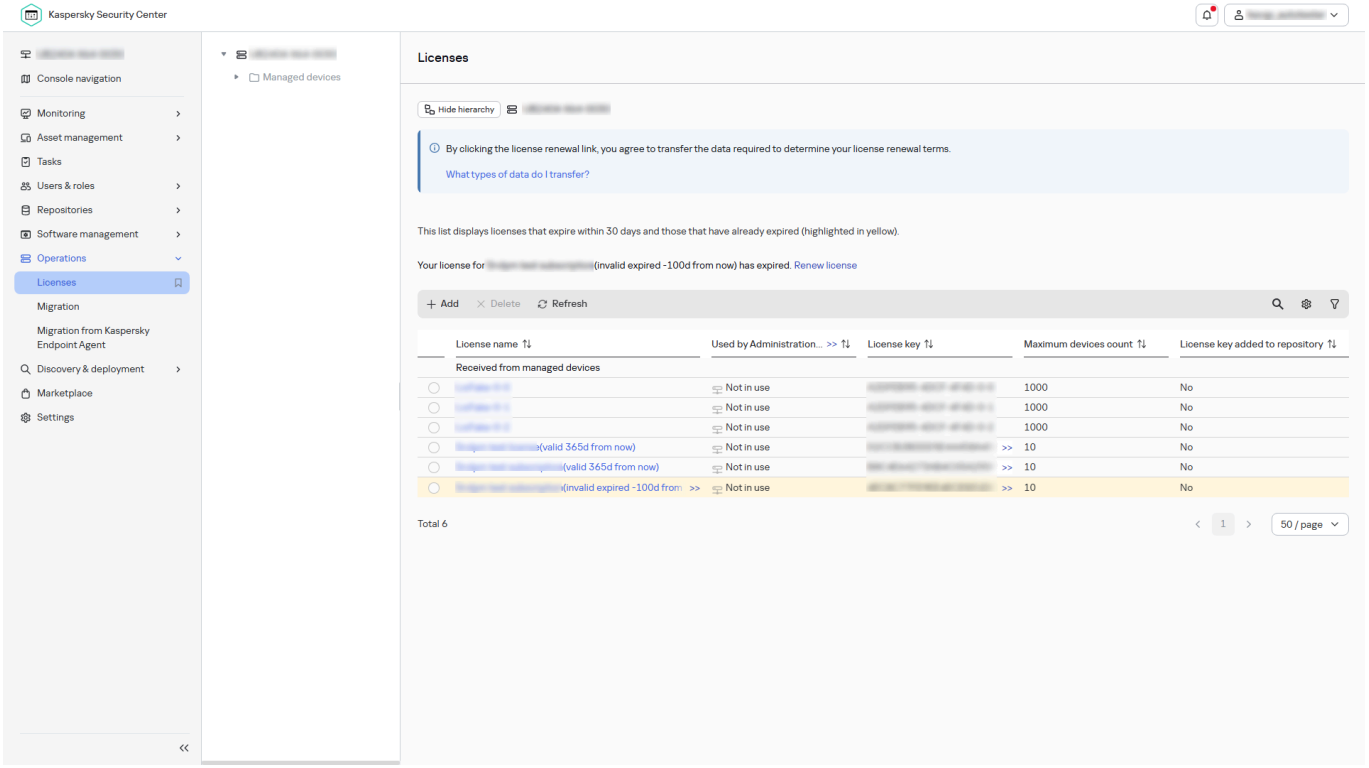
Добавление кода активации или файла ключа вручную на устройства

Вы можете активировать установленное приложение "Лаборатории Касперского" локально, используя инструменты приложения. Дополнительную информацию см. в документации к установленным приложениям.

Добавление лицензионного ключа в хранилище Сервера администрирования

Чтобы добавить лицензионный ключ в хранилище Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Операции** → **Лицензии**.



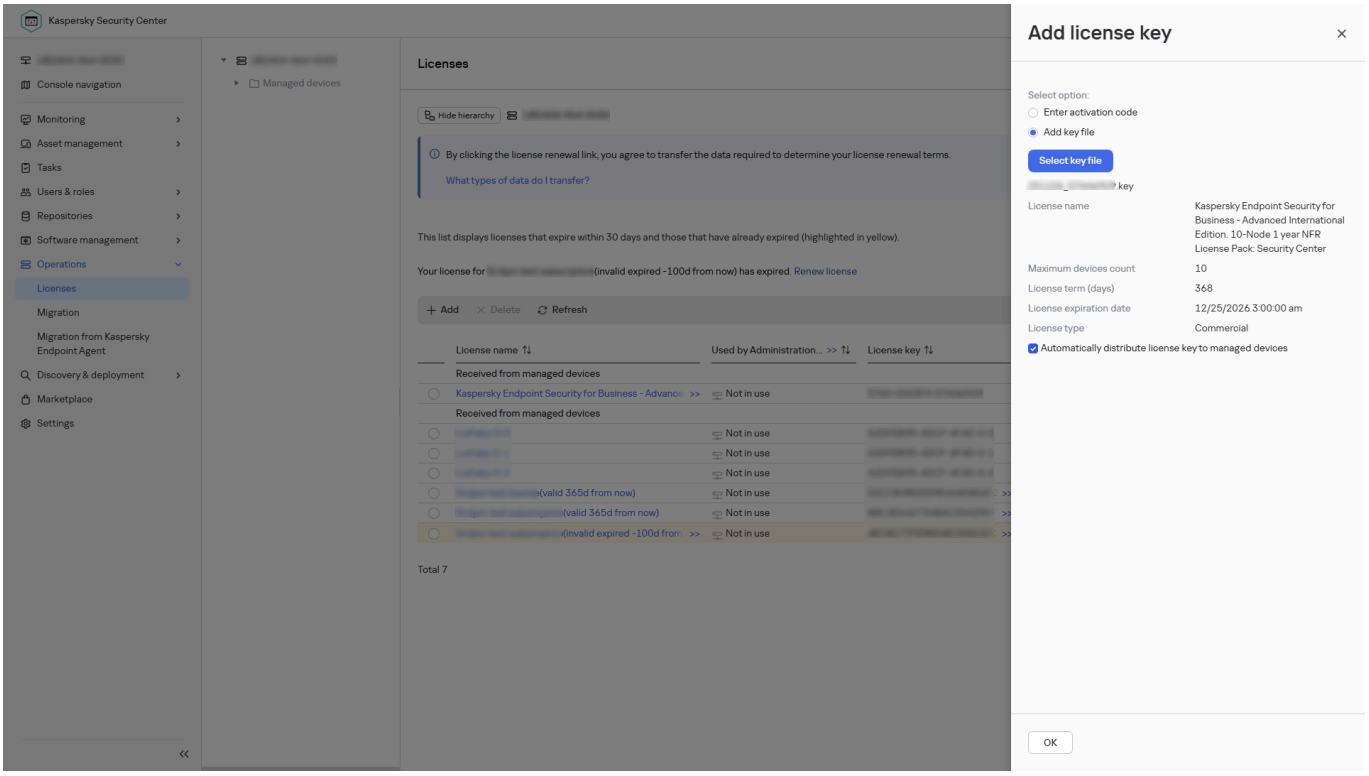
Список добавленных лицензионных ключей "Лаборатории Касперского"

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.



Добавление лицензионного ключа путем применения файла ключа

- **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 Web Console позволяет распространить лицензионный ключ на клиентские устройства автоматически или с помощью задачи **Активация приложения**. Вы можете использовать задачу для распространения ключей в определенной группе устройств. При распространении лицензионного ключа с помощью задачи учитывается лицензионное ограничение на количество устройств. Используйте автоматическое распространение ключей, чтобы автоматически прекратить распространение лицензионного ключа при достижении лицензионного ограничения.

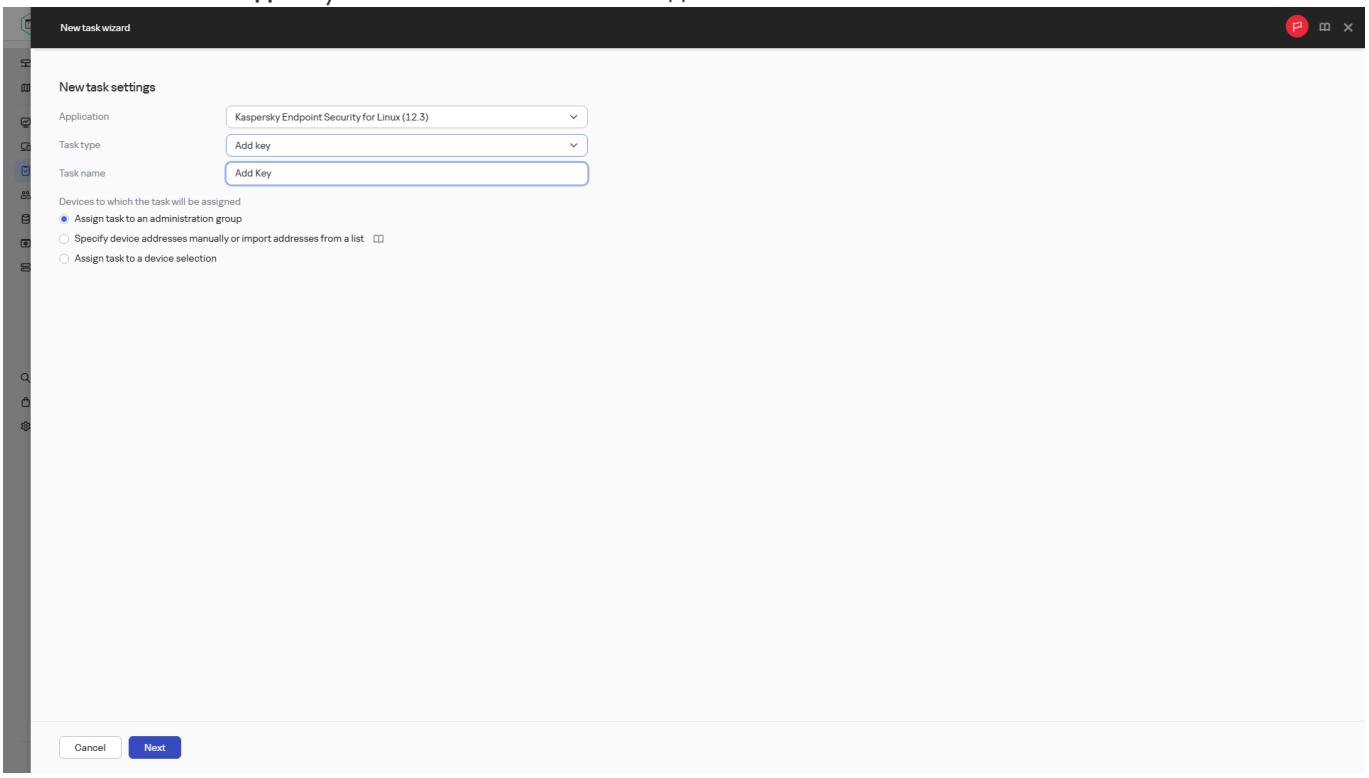
Если вы включили автоматическое распространение лицензионного ключа, не создавайте задачу **Активация приложения** для распространения этого ключа на клиентские устройства. Иначе нагрузка на Сервер администрирования увеличится из-за частой синхронизации.

Перед распространением добавьте лицензионный ключ в хранилище Сервера администрирования.

*Чтобы распространить лицензионный ключ на клиентские устройства с помощью задачи **Активация приложения**:*

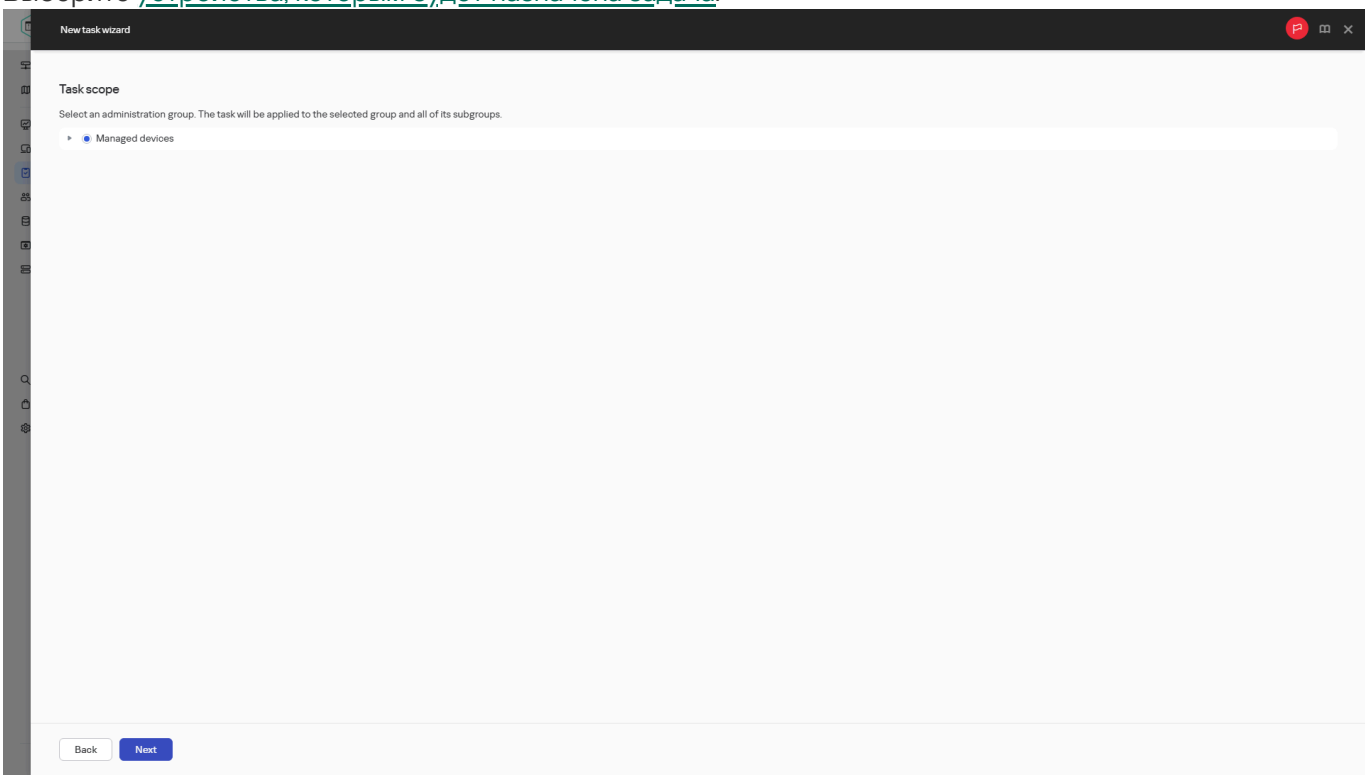
1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится **мастер создания задачи**. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В раскрывающемся списке **Приложение** выберите приложение, для которого вы хотите добавить лицензионный ключ.
4. В списке **Тип задачи** выберите задачу **Активация приложения**.
5. В поле **Название задачи** укажите название новой задачи.



Создание задачи добавления ключа

6. Выберите устройства, которым будет назначена задача.



Указание области действия задачи

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 **Активация приложения**.

- Выберите параметр **Ввести код активации**, чтобы ввести код активации, а затем выполните следующие действия:

  a. Укажите код активации и нажмите на кнопку **Отправить**.

  Информация о лицензионном ключе отображается в панели добавления ключа.

  b. Нажмите на кнопку **Сохранить**.

  > Если вы хотите автоматически распространять лицензионный ключ на управляемые устройства, включите параметр **Автоматически распространять лицензионный ключ на управляемые устройства**.

  Панель добавления ключа закрыта.

- Выберите параметр **Добавить файл ключа**, чтобы добавить файл ключа, и выполните следующие действия:

  a. Нажмите на кнопку **Выберите файл ключа**.

  b. В открывшемся окне выберите файл ключа и нажмите на кнопку **Открыть**.

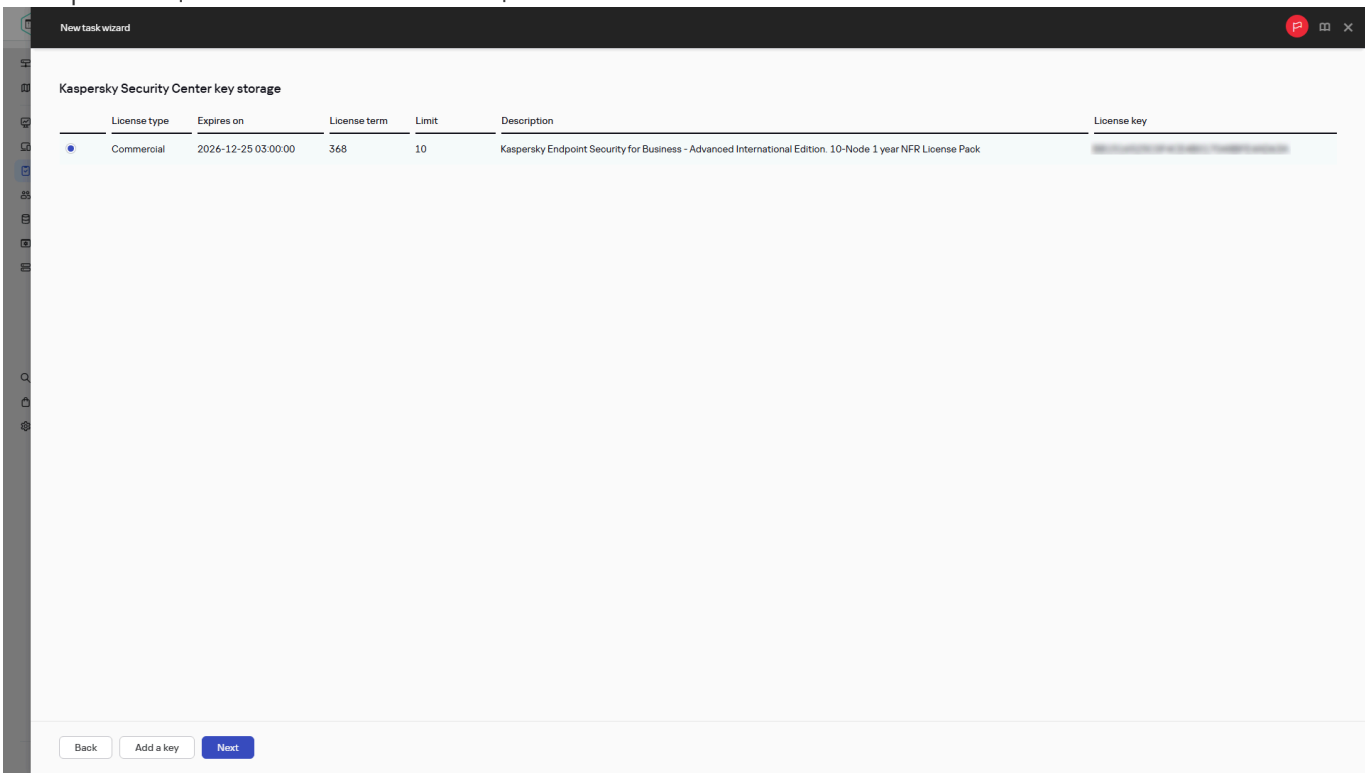
  Информация о лицензионном ключе отображается в панели добавления лицензионного ключа.

  c. Нажмите на кнопку **Сохранить**.

  > Если вы хотите автоматически распространять лицензионный ключ на управляемые устройства, включите параметр **Автоматически распространять лицензионный ключ на управляемые устройства**.

  Панель добавления ключа закрыта.

9. Выберите лицензионный ключ в таблице ключей.

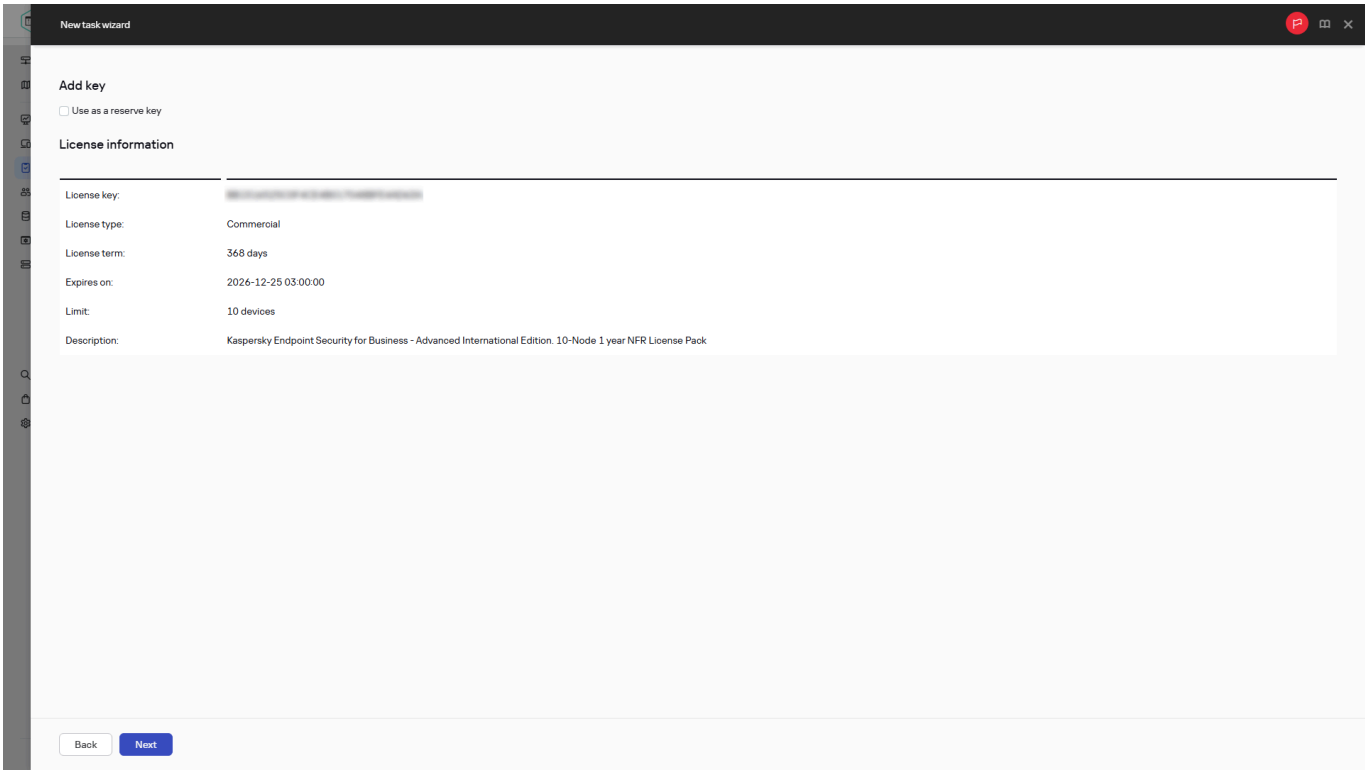


Выбор лицензионного ключа

10. Если вы хотите заменить активный лицензионный ключ, на шаге мастера **Информация о лицензии** снимите флажок **Использовать в качестве резервного лицензионного ключа**.

    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.



Указание резервного лицензионного ключа

11. Если на шаге мастера **Завершение создания задачи** включить параметр **Открыть окно свойств задачи после ее создания**, вы сможете изменить установленные по умолчанию значения параметров задачи.

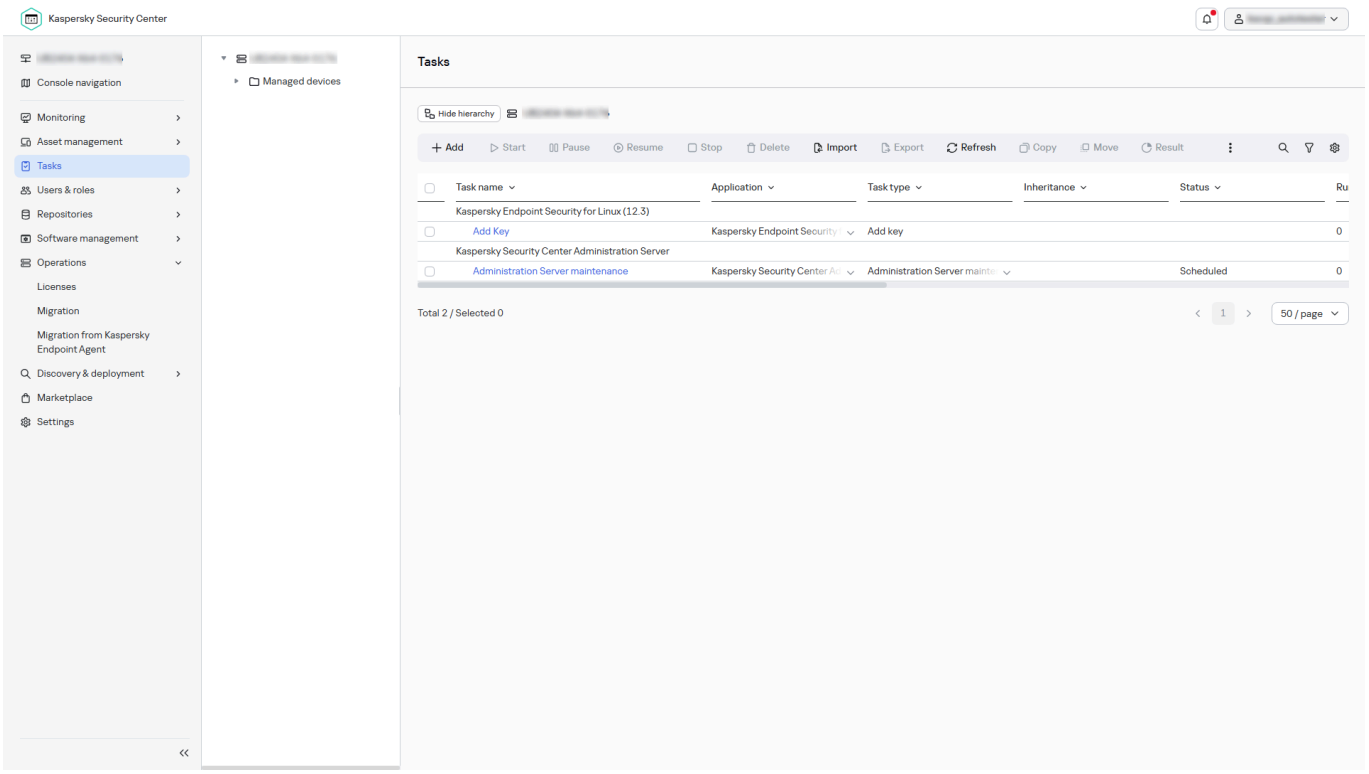
    Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже.

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.



Список 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.

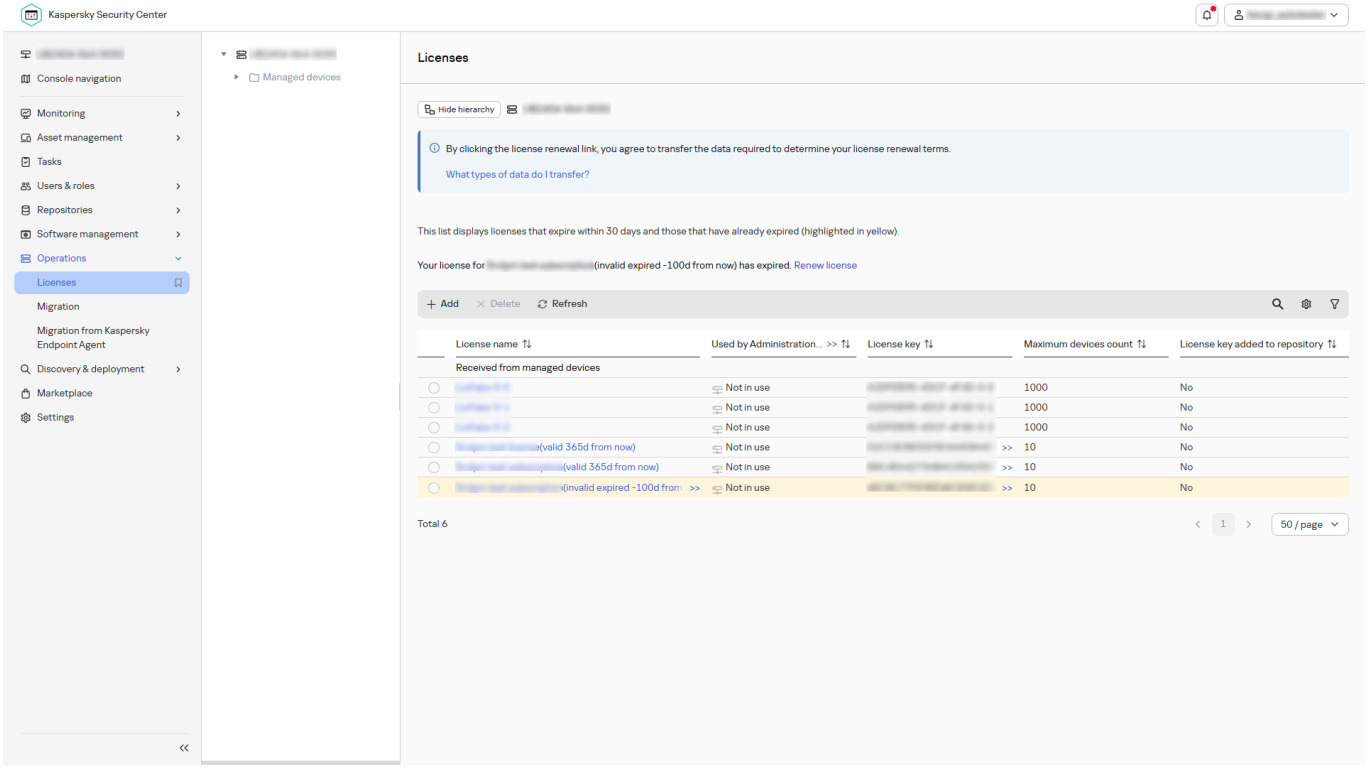
После завершения задачи, лицензионный ключ распространится на выбранные устройства.

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:

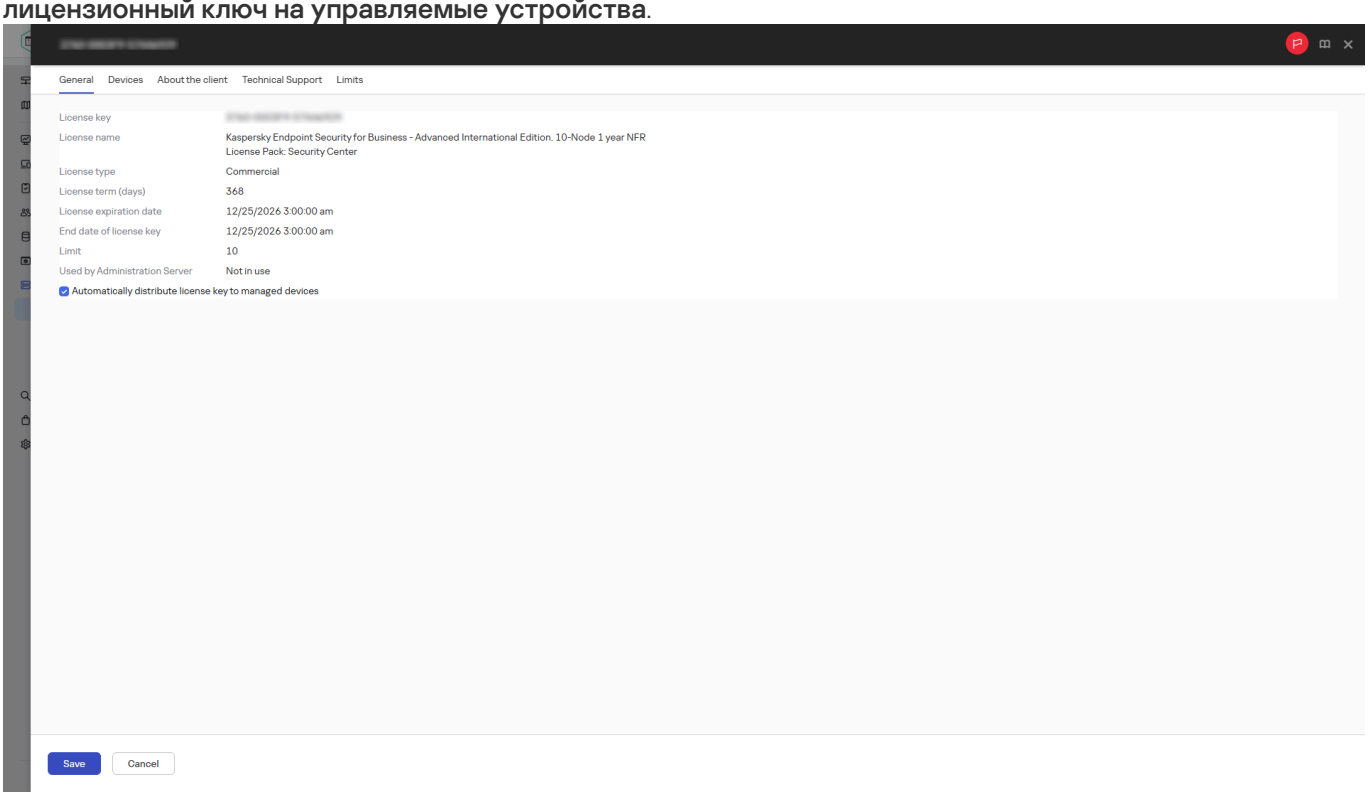
1. В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии**.



Список лицензий

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**.



Окно свойств лицензионного ключа

4. Нажмите на кнопку **Сохранить**.

Лицензионный ключ будет автоматически распространяться на те устройства, для которых он подходит.

Распространение лицензионного ключа выполняется средствами Агента администрирования. Задачи распространения резервного лицензионного ключа для приложения при этом не создаются.

При автоматическом распространении лицензионного ключа учитывается лицензионное ограничение на количество устройств. Лицензионное ограничение задано в свойствах лицензионного ключа. Если лицензионное ограничение достигнуто, распространение лицензионного ключа на устройства автоматически прекращается.

Обратите внимание, что автоматически распространяемый лицензионный ключ может не отображаться в хранилище виртуального Сервера администрирования в следующих случаях:

- Лицензионный ключ недействителен для приложения.
- Виртуальный Сервер администрирования не имеет управляемых устройств.
- Лицензионный ключ уже используется для устройств, управляемых другим виртуальным Сервером администрирования, и достигнуто лицензионное ограничение на количество устройств.

Виртуальный Сервер администрирования автоматически распространяет лицензионные ключи из своего хранилища и из хранилища Сервера администрирования. Рекомендуется:

- Используйте задачу *Добавить лицензионный ключ*, чтобы выбрать лицензионный ключ, который необходимо развернуть на устройствах.
- Не выключайте параметр **Разрешить автоматическое распространение лицензионных ключей этого виртуального Сервера на его устройства** в параметрах виртуального Сервера администрирования. Иначе виртуальный Сервер администрирования не будет распространять лицензионные ключи на устройства, в том числе лицензионные ключи из хранилища Сервера администрирования.

Если 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 приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии**.

Отобразится список файлов ключей и кодов активации, добавленных в хранилище Сервера администрирования.

Чтобы просмотреть подробную информацию о лицензионном ключе:

1. В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии**.
2. Нажмите на имя требуемого лицензионного ключа.

В открывшемся окне свойств лицензионного ключа вы можете просмотреть:

- На вкладке **Общие** – основную информацию о лицензионном ключе.
- На вкладке **Устройства** – список клиентских устройств, на которых использовался лицензионный ключ для активации установленного приложения "Лаборатории Касперского".
- На вкладке **Ограничения** – список лицензионных ограничений.

  Если вы активировали Сервер администрирования по лицензии Kaspersky Security для бизнеса Профессиональный, на вкладке **Ограничения** отображается поле **XDR-O** со значением **Включено**.

Чтобы просмотреть, какие лицензионные ключи распространены на выбранное клиентское устройство:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.
2. Нажмите на имя требуемого устройства.

3. В открывшемся окне свойств устройства выберите вкладку **Приложения**.

4. Нажмите на название приложения, для которого вы хотите просмотреть информацию о распространенном лицензионном ключе.

5. В открывшемся окне свойств приложения перейдите на вкладку **Общие** и откройте раздел **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. Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы.

События превышения лицензионного ограничения

Kaspersky Security Center Linux позволяет получать информацию о событиях превышения лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах.

Уровень важности событий о превышении лицензионного ограничения определяется по следующим правилам:

- Если количество используемых лицензионных единиц одной лицензии лежит в интервале 90–100% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Информационное сообщение**.
- Если количество используемых лицензионных единиц одной лицензии лежит в интервале 100–110% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Предупреждение**.
- Если количество используемых лицензионных единиц одной лицензии превышает 110% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Критическое событие**.

Удаление лицензионного ключа из хранилища

При удалении активного лицензионного ключа, который распространен на управляемые устройства, приложения продолжают работать на управляемых устройствах.

Чтобы удалить файл ключа или код активации из хранилища Сервера администрирования:

1. Убедитесь, что Сервер администрирования не использует файл ключ или код активации, который вы хотите удалить. Если Сервер администрирования использует такой ключ, вы не сможете удалить ключ. Чтобы выполнить проверку:

   a. В главном окне приложения нажмите на имя Сервера администрирования.

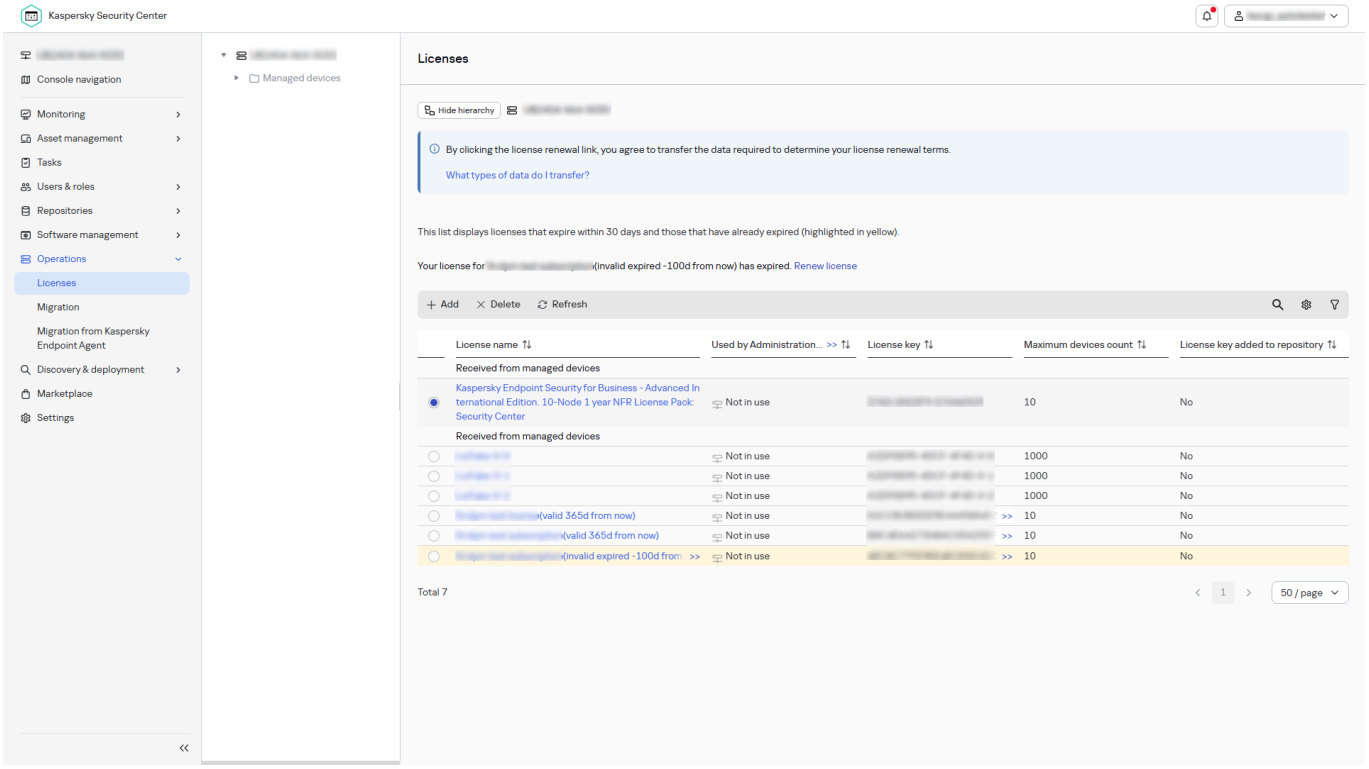
      Откроется окно свойств Сервера администрирования.

b. На вкладке **Общие** выберите раздел **Лицензионные ключи**.

c. Если в открывшемся разделе отображается требуемый файл ключ или код активации, нажмите на кнопку **Удалить активный лицензионный ключ** и подтвердите операцию. После этого Сервер администрирования не использует удаленный лицензионный ключ, ключ остается в хранилище Сервера администрирования. Если требуемый файл ключ или код активации не отображается, Сервер администрирования его не использует.

2. В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии**.

3. Выберите нужный файл ключа или код активации и нажмите на кнопку **Удалить**.



Список лицензий

Выбранный файл ключа или код активации удален из хранилища.

Можно добавить удаленный лицензионный ключ повторно или добавить другой лицензионный ключ.

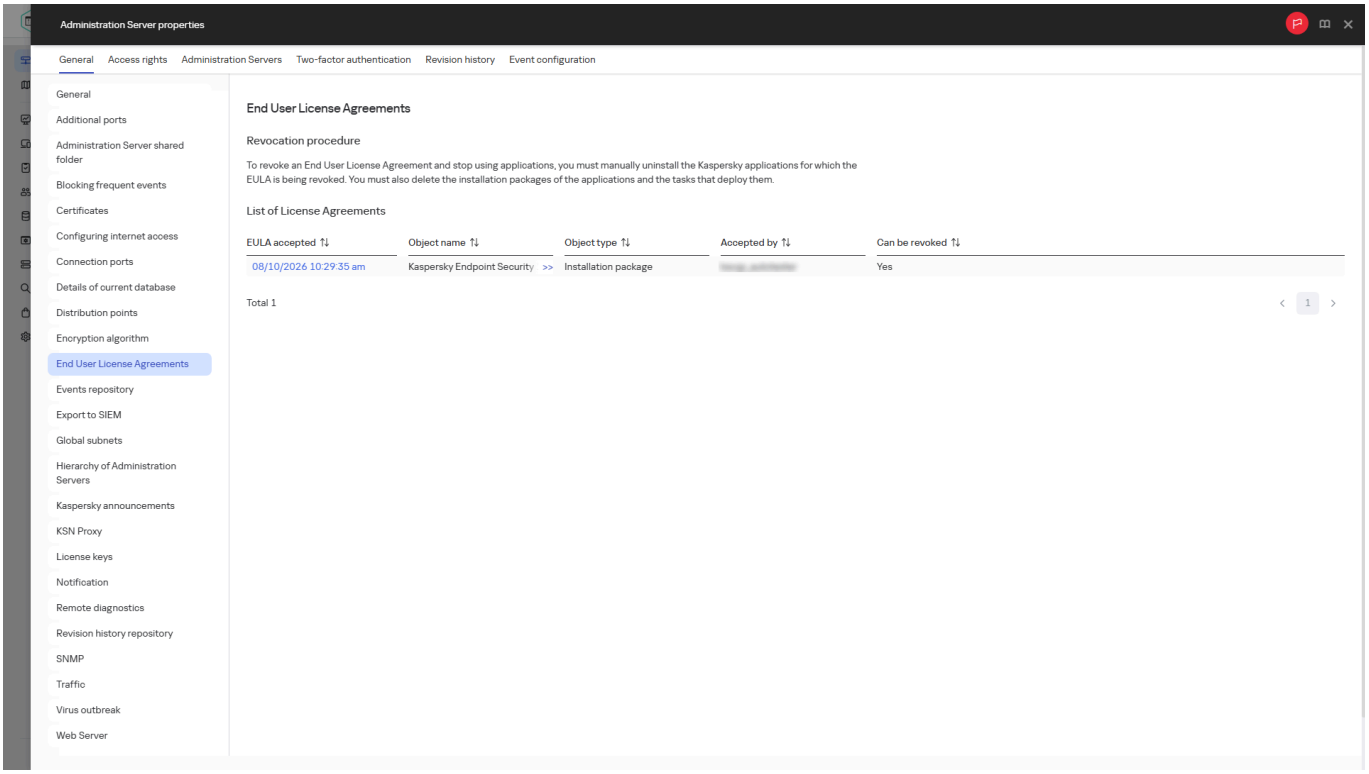
Отзыв согласия с Лицензионным соглашением

Если вы решите прекратить защиту некоторых своих клиентских устройств, вы можете отозвать Лицензионное соглашение для любого управляемого приложения "Лаборатории Касперского". Вам нужно удалить выбранное приложение, прежде чем отзывать его Лицензионное соглашение.

Чтобы отозвать Лицензионное соглашение для управляемых приложений "Лаборатории Касперского":

1. Откройте окно свойств Сервера администрирования и на вкладке **Общие** выберите раздел **Лицензионные соглашения**.

Отобразится список Лицензионных соглашений, принятых при создании инсталляционных пакетов, установке обновлений или развертывании Kaspersky Security для мобильных устройств.



Список Лицензионных соглашений

2. В списке выберите Лицензионные соглашения, которые вы хотите отозвать.

   Можно просмотреть следующие свойства Лицензионных соглашений:

   - Дата принятия Лицензионного соглашения.
   - Имя пользователя, принявшего Лицензионное соглашение.

3. Нажмите на дату принятия любого Лицензионного соглашения, чтобы открыть окно его свойств, в котором отображаются следующие данные:

   - Имя пользователя, принявшего Лицензионное соглашение.
   - Дата принятия Лицензионного соглашения.
   - Уникальный идентификатор (UID) Лицензионного соглашения.
   - Полный текст Лицензионного соглашения.
   - Список объектов (инсталляционных пакетов, обновлений, мобильных приложений), связанных с Лицензионным соглашением, и их соответствующие имена и типы.

4. В нижней части окна свойств Лицензионного соглашения нажмите на кнопку **Отозвать Лицензионное соглашение**.

   Если существуют какие-либо объекты (инсталляционные пакеты и их соответствующие задачи), которые не позволяют отозвать Лицензионное соглашение, отображается соответствующее уведомление. Вы не можете продолжить отзыв, пока не удалите эти объекты.

В открывшемся окне отобразится сообщение о том, что сначала необходимо удалить приложение "Лаборатории Касперского", которому соответствует это Лицензионное соглашение.

5. Нажмите на кнопку, подтверждающую отзыв лицензии.

Лицензионное соглашение отозвано. Лицензионное соглашение больше не отображается в списке Лицензионных соглашений в разделе **Лицензионные соглашения**. Окно свойств Лицензионного соглашения закрывается; приложение больше не установлено.

Продление срока действия лицензии приложений "Лаборатории Касперского"

Вы можете продлить срок действия лицензии приложений "Лаборатории Касперского", срок действия которой истек или скоро истечет (менее чем через 30 дней).

Чтобы продлить срок действия лицензии, который истекает или уже истек:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии**.
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга** и перейдите по ссылке **Просмотреть лицензии, срок действия которых истек** рядом с уведомлением.

   Откроется окно **Лицензии**, 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 Linux: версию, локализацию, которую вы используете, идентификатор лицензии на программное обеспечение (то есть идентификатор лицензии, которую вы продлеваете), а также то, приобрели ли вы лицензию через компанию-партнера или нет.

3. В открывшемся окне продления срока действия лицензии следуйте инструкциям.

   Срок действия лицензии продлен.

В Kaspersky Security Center Web Console уведомления отображаются при приближении истечения срока действия лицензии по следующему расписанию:

- за 30 дней до истечения срока действия;
- за 7 дней до истечения срока действия;
- за 3 дней до истечения срока действия;
- за 24 часа до истечения срока действия;
- когда срок действия лицензии истек.

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 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 сервисы.
  - **Сеть**: локальная сеть, ИТ-инфраструктура.
  - **Услуга**: услуги, связанные с безопасностью, предоставляемые "Лабораторией Касперского".

Чтобы найти и приобрести бизнес-решение "Лабораторией Касперского":

1. В главном окне приложения перейдите в раздел **Marketplace**.

   По умолчанию в разделе отображаются все доступные бизнес-решения "Лаборатории Касперского".

2. Чтобы просмотреть только те решения, которые подходят вашей организации, выберите нужные значения в фильтрах.

3. Нажмите на решение, которое вы хотите приобрести или о котором хотите узнать больше.

Вы будете перенаправлены на веб-страницу решения. Следуйте инструкциям на экране, чтобы перейти к покупке.

Настройка приложений "Лаборатории Касперского"

В этом разделе содержится информация о настройке вручную политик и задач, о ролях пользователей, о построении структуры групп администрирования и об иерархии задач.

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 Linux.
- Установили Kaspersky Security Center Web Console.
- Выполнили основной сценарий установки Kaspersky Security Center Linux.
- 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;
  - задача *Поиск уязвимостей и требуемых обновлений*.

Этапы

Настройка защиты сети состоит из следующих этапов:

1. **Настройка и распространение политик и профилей политик для приложений "Лаборатории Касперского"**

   Для настройки и распространения параметров приложений "Лаборатории Касперского", установленных на управляемых устройствах, можно использовать два различных подхода управления безопасностью: ориентированный на пользователей и ориентированный на устройства. Можно комбинировать эти два подхода.

2. **Настройка задач для удаленного управления приложениями "Лаборатории Касперского"**

   Проверьте задачи, созданные с помощью мастера первоначальной настройки, и при необходимости оптимизируйте их параметры.

   Инструкции: Настройка групповой задачи обновления Kaspersky Endpoint Security, Создание задачи Поиск уязвимостей и требуемых обновлений.

   При необходимости создайте дополнительные задачи управления приложениями "Лаборатории Касперского", установленными на клиентских устройствах.

3. **Оценка и ограничение загрузки событий в базу данных**

   Информация о событиях, которые возникают во время работы управляемых приложений, передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

   Инструкции: Настройка количества событий в хранилище событий.

Результаты

После завершения этого сценария ваша сеть будет защищена благодаря настройке приложений "Лаборатории Касперского", задач и событий, получаемых Сервером администрирования:

- Приложения "Лаборатории Касперского" настроены в соответствии с политиками и профилями политик.
- Управление приложениями осуществляется с помощью набора задач.
- Задано максимальное количество событий, которые могут храниться в базе данных.

После завершения настройки защиты сети вы можете приступить к настройке регулярных обновлений баз и приложений "Лаборатории Касперского".

Подходы к управлению безопасностью, ориентированные на устройства и на пользователей

Вы можете управлять параметрами безопасности с позиции функций устройства и с позиции пользовательских ролей. Первый подход называется *управление безопасностью, ориентированное на устройства*, второй подход называется *управление безопасностью, ориентированное на пользователей*. Чтобы применить разные параметры приложений к разным устройствам, вы можете использовать один или оба типа управления в комбинации.

Управление безопасностью, ориентированное на устройства, позволяет вам применять различные параметры приложения безопасности к управляемым устройствам в зависимости от особенностей устройства. Например, вы можете применить различные параметры к устройствам, которые размещены в разных группах администрирования.

Управление безопасностью, ориентированное на пользователя, позволяет вам применять различные параметры приложений безопасности к различным ролям пользователей. Вы можете создать несколько пользовательских ролей, назначить соответствующую пользовательскую роль каждому пользователю и определить различные параметры приложения для устройств, принадлежащих пользователям с различными ролями. Например, можно применить различные параметры приложений к устройствам бухгалтеров и к устройствам специалистов отдела кадров. В результате внедрения управления безопасностью, ориентированного на пользователей, каждый отдел – отдел бухгалтерии и отдел кадров – получит свою собственную конфигурацию параметров для работы с приложениями "Лаборатории Касперского". Конфигурация параметров определяет, какие параметры приложения могут быть изменены пользователями, а какие принудительно установлены и заблокированы администратором.

Управление безопасностью, ориентированное на пользователей, позволяет применять заданные параметры приложений для отдельных пользователей. Это может потребоваться, если сотруднику назначена уникальная роль в организации или если требуется проконтролировать проблемы безопасности, связанные с определенным сотрудником. В зависимости от роли этого сотрудника в компании, можно расширить или сократить его права, чтобы изменить параметры приложения. Например, может потребоваться расширить права системного администратора, управляющего клиентскими устройствами в локальном офисе.

Вы также можете комбинировать подходы к управлению безопасностью, ориентированные на пользователей и ориентированные на устройства. Например, можно настроить разные политики для каждой группы администрирования, а затем дополнительно создать профили политик 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 приоритетами профилей политик.
3. Политики модифицируются профилями политик, связанными с ролями пользователей.

Настройка и распространение политик: подход, ориентированный на устройства

После завершения этого сценария приложения будут настроены на всех управляемых устройствах в соответствии с политиками приложений и профилями политики, которые вы определяете.

Предварительные требования

Убедитесь, что вы установили Сервер администрирования Kaspersky Security Center Linux и Kaspersky Security Center 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 приложениями "Лаборатории Касперского", ориентированный на устройства, содержит следующие шаги:

1. **Настройка политик приложений**

   Настройте параметры установленных приложений "Лаборатории Касперского" на управляемых устройствах с помощью создания политики для каждого приложения. Этот набор политик будет применен к клиентским устройствам.

   При настройке защиты сети с помощью мастера первоначальной настройки Kaspersky Security Center Linux создает политику по умолчанию для следующих приложений:

   - Kaspersky Endpoint Security для Linux – для клиентских устройств с операционной системой Linux.
   - Kaspersky Endpoint Security для Windows – для клиентских устройств с операционной системой Windows.

   Если вы завершили процесс настройки с помощью этого мастера, вам не нужно создавать новую политику для этого приложения.

   Если у вас иерархическая структура нескольких Серверов администрирования и/или групп администрирования, подчиненные Серверы администрирования и дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами и подчиненными Серверами администрирования, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их выше по иерархии политики. Остальные незаблокированные параметры будут доступны для изменения в политике ниже по иерархии. Созданная иерархия политик позволяет эффективно управлять устройствами в группах администрирования.

   Инструкция: Создание политики.

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 приложения "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 приложениям "Лаборатории Касперского".

   Вы можете проверить, доставлены ли политики и профили политик на устройство. Kaspersky Security Center Linux определяет дату и время доставки в свойствах устройства.

   Инструкции: Принудительная синхронизация

Результаты

После завершения сценария, ориентированного на устройства, приложения "Лаборатории Касперского" будут настроены в соответствии с параметрами, указанными и распространенными через иерархию политик.

Политики приложений и профили политик будут автоматически применяться к новым устройствам, добавленным в группы администрирования.

Настройка и распространение политик: подход, ориентированный на пользователя

В этом разделе описывается сценарий, ориентированный на пользователя для централизованной настройке приложений "Лаборатории Касперского", установленных на управляемых устройствах. После завершения этого сценария приложения будут настроены на всех управляемых устройствах в соответствии с политиками приложений и профилями политики, которые вы определяете.

Предварительные требования

Убедитесь, что вы успешно установили Сервер администрирования Kaspersky Security Center Linux и Kaspersky Security Center 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 приложениями "Лаборатории Касперского", ориентированный на пользователя, содержит следующие шаги:

1. **Настройка политик приложений**

   Настройте параметры установленных приложений "Лаборатории Касперского" на управляемых устройствах с помощью создания политики для каждого приложения. Этот набор политик будет применен к клиентским устройствам.

   При настройке защиты сети с помощью мастера первоначальной настройки Kaspersky Security Center Linux создает политику по умолчанию для Kaspersky Endpoint Security. Если вы завершили процесс настройки с помощью этого мастера, вам не нужно создавать новую политику для этого приложения.

   Если у вас иерархическая структура нескольких Серверов администрирования и/или групп администрирования, подчиненные Серверы администрирования и дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами и подчиненными Серверами администрирования, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их выше по иерархии политики. 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. Вам нужно разделить всех сотрудников в соответствии с их ролями. Например, вы можете разделить их по отделам, профессиям или должностям. После этого вам потребуется создать роль пользователя для каждой группы. В этом случае каждая пользовательская роль будет иметь свой собственный профиль политики, содержащий параметры приложения, специфичные для этой роли.

4. **Создание пользовательских ролей**

   Создайте и настройте пользовательскую роль для каждой группы сотрудников, которую вы определили на предыдущем шаге, или используйте предопределенные роли. Роли пользователей содержат набор прав доступа к функциям приложения.

   Инструкция: Создание роли пользователя.

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 профилей политики**

   Создайте профиль политики для каждой роли пользователя вашей организации. Профили политики определяют, какие параметры должны применяться к приложениям, установленным на устройствах пользователей, в зависимости от роли каждого пользователя.

   Инструкция: Создание профиля политики.

7. **Связь профиля политики с ролями пользователей**

   Свяжите созданные профили политики с ролями пользователей. После чего, профиль политики становится активным для пользователей, которым определена эта роль. Параметры профиля политики, применяются к приложениям "Лаборатории Касперского", установленным на устройствах пользователя.

   Инструкция: связь профилей политики с ролями.

8. **Распространение политик и профилей политик на управляемые устройства**

   По умолчанию синхронизация Kaspersky Security Center Linux с Сервером администрирования происходит раз в 15 минут. Во время синхронизации новые или измененные политики и профили политик применяются к управляемым устройствам. Вы можете пропустить автоматическую синхронизацию и запустить синхронизацию вручную с помощью команды Синхронизировать принудительно. После завершения синхронизации политики и профили политик доставляются и применяются к установленным приложениям "Лаборатории Касперского".

   Вы можете проверить, доставлены ли политики и профили политик на устройство. Kaspersky Security Center Linux определяет дату и время доставки в свойствах устройства.

   Инструкции: Принудительная синхронизация

Результаты

После завершения сценария, ориентированного на пользователя, приложения "Лаборатории Касперского" будут настроены в соответствии с параметрами, указанными и распространенными через иерархию политик и профили политик.

Для нового пользователя вам необходимо создать учетную запись, назначить пользователю одну из созданных пользовательских ролей и назначить устройства пользователю. Политики приложений и профили политик будут автоматически применяться к устройствам этого пользователя.

Политики и профили политик

В Kaspersky Security Center Web Console можно создавать политики для приложений "Лаборатории Касперского". В этом разделе описаны политики и профили политик, а также приведены инструкции по их созданию и изменению.

О политиках и профилях политик

Политика – это набор параметров приложения "Лаборатории Касперского", которые применяются к группе администрирования и ее подгруппе. Вы можете установить несколько приложений "Лаборатории Касперского" на устройства группы администрирования. Kaspersky Security Center предоставляет по одной политике для каждого приложения "Лаборатории Касперского" в группе администрирования. Политика имеет один из следующих статусов:

Статус политики

Состояние	Описание
Активная	Это текущая политика, которая применяется к устройству. Для приложения "Лаборатории Касперского" в каждой группе администрирования может быть активна только одна политика. Значения параметров активной политики приложения "Лаборатории Касперского" применяются к устройству.
Неактивная	Политика, которая в настоящее время не применяется к устройству.
Для автономных пользователей	Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.

Политики действуют по следующим правилам:

- Для одного приложения можно настроить несколько политик с различными значениями.
- Для одного приложения может быть активна только одна политика.
- Политика может иметь дочерние политики.

Вы можете использовать политики для подготовки к экстренным ситуациям, например, к вирусной атаке. Например, если происходит атака через флеш-накопители USB, можно активировать политику, блокирующую доступ к флеш-накопителям. В этом случае текущая активная политика автоматически становится неактивной.

Чтобы не поддерживать большое число политик, например, когда в разных случаях предполагается изменение только нескольких параметров, вы можете использовать профили политик.

Профиль политики – это именованное подмножество параметров политики, которые заменяют значения параметров политики. Профиль политики влияет на формирование эффективных параметров управляемого устройства. *Эффективные параметры* – это набор параметров политики, параметров профиля политики и параметров локального приложения, которые в настоящее время применяются к устройству.

Профили политик работают по следующим правилам:

- Профиль политики вступает в силу при возникновении определенного условия активации.
- Профили политики содержат значения параметров, которые отличаются от параметров политики.
- Активация профиля политики изменяет эффективные параметры управляемого устройства.
- В политике может быть не более 100 профилей политик.

Блокировка (замок) и заблокированные параметры

У каждого параметра политики есть значок замка (🔒). В таблице ниже показаны состояния значка замка:

Статусы значка замка

Состояние	Описание
Undefined	Если рядом с параметром отображается значок открытого замка и переключатель выключен, параметр не указан в политике. Пользователь может изменить эти параметры в интерфейсе управляемого приложения. Такие параметры называются *разблокированными*.
Enforce	Если рядом с параметром отображается закрытый значок замка и переключатель включен, параметр применяется к устройствам, на которых применяется политика. Пользователь не может изменять значения этих параметров в интерфейсе управляемого приложения. Такие параметры называются *заблокированными*.

Рекомендуется заблокировать параметры политики, которые вы хотите применить к управляемым устройствам. Разблокированные параметры политики могут быть переназначены параметрами приложения "Лаборатории Касперского" на управляемом устройстве.

Вы можете использовать значок замка для выполнения следующих действий:

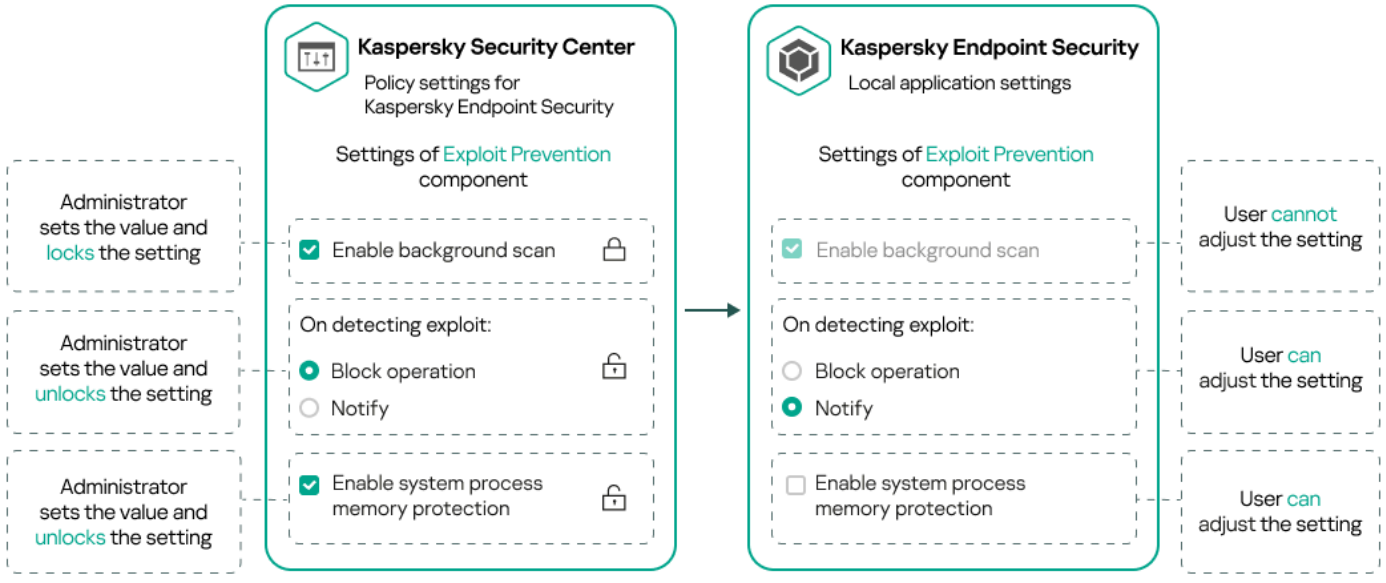
- Блокировка параметров для политики подгруппы администрирования.
- Блокировка параметров приложения "Лаборатории Касперского" на управляемом устройстве.

Таким образом, заблокированный параметр используется в эффективных параметрах на управляемом устройстве.

Применение эффективных параметров включает в себя следующие действия:

- Управляемое устройство применяет значения параметров приложения "Лаборатории Касперского".
- Управляемое устройство применяет заблокированные значения параметров политики.

Политика и управляемое приложение "Лаборатории Касперского" содержат одинаковый набор параметров. При настройке параметров политики параметры приложения "Лаборатории Касперского" меняют значения на управляемом устройстве. Вы не можете изменить заблокированные параметры на управляемом устройстве (см. рисунок ниже):



Замки и параметры приложения "Лаборатории Касперского"

Наследование политик и профилей политик

В этом разделе представлена информация об иерархии и наследовании политик и профилей политик.

Иерархия политик

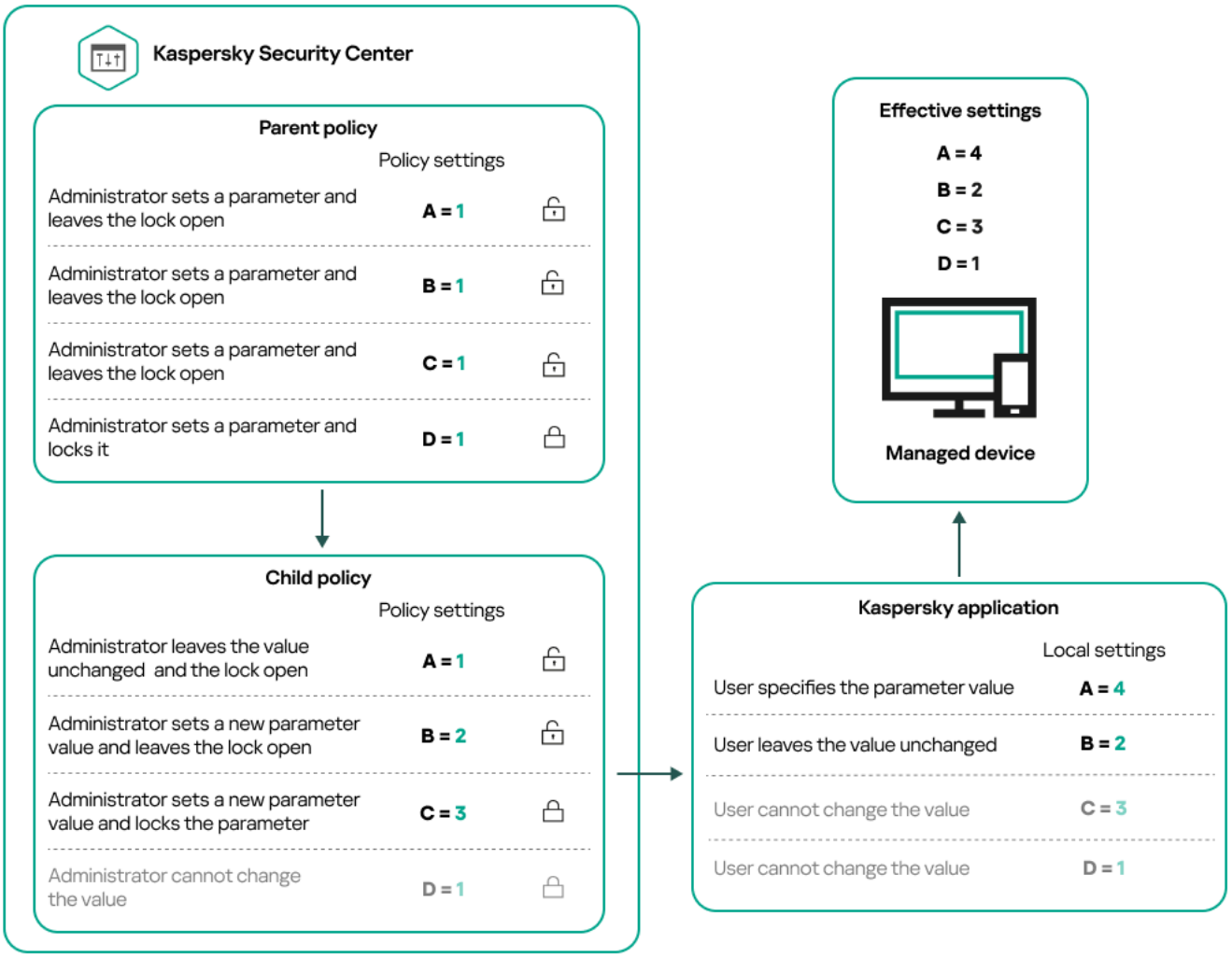
Если для разных устройств требуются разные параметры, вы можете объединить устройства в группы администрирования.

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 одного и того же приложения действуют друг на друга по иерархии групп администрирования. Заблокированные параметры из политики вышестоящей (родительской) группы администрирования будут переназначать значения параметров политики подгруппы (см. рисунок ниже).

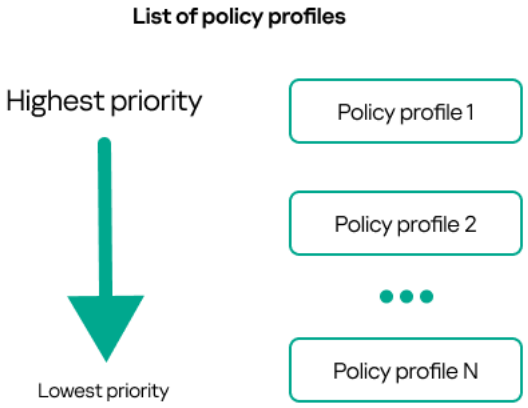


Иерархия политик

Профили политик в иерархии политик

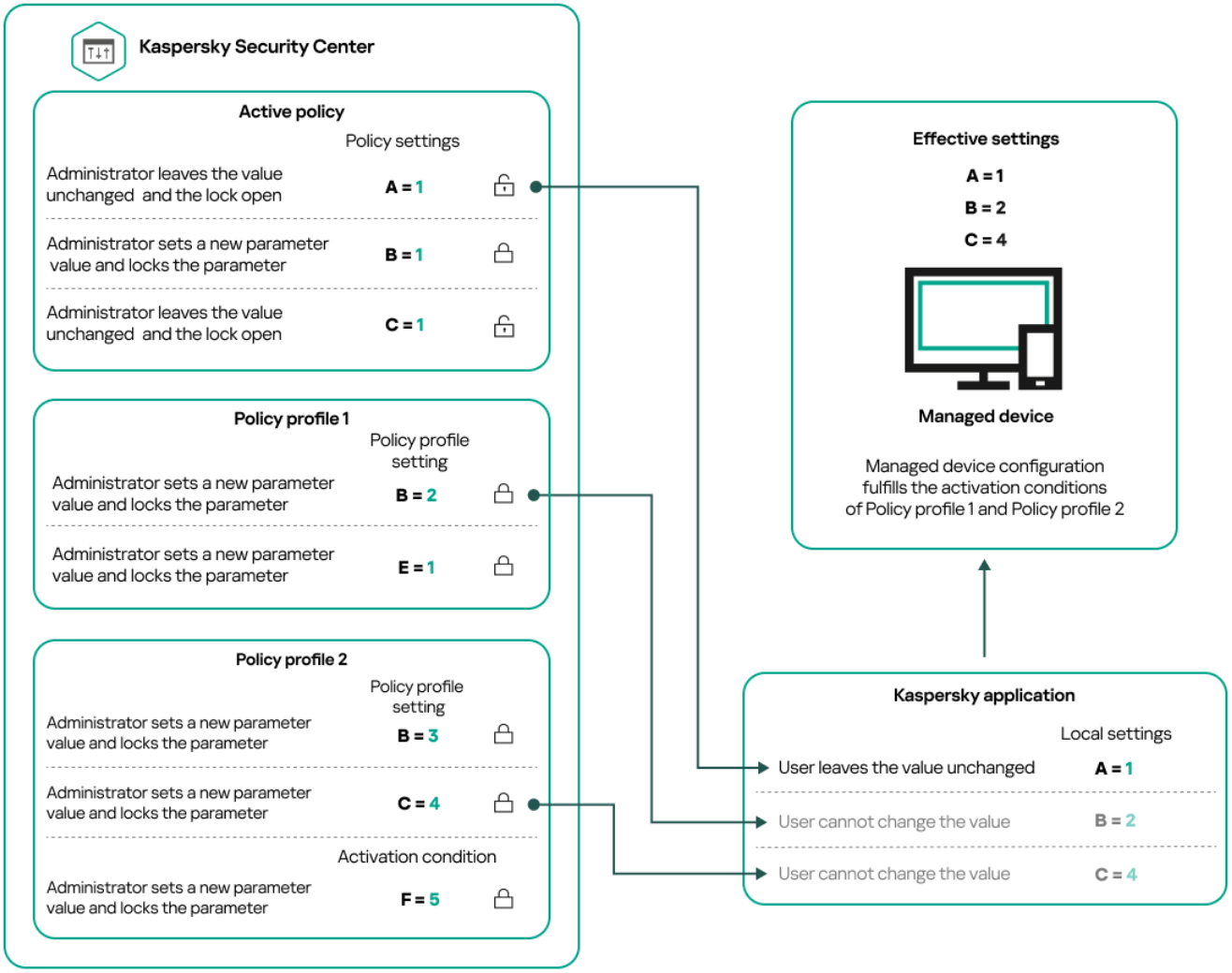
Профили политики имеют следующие условия назначения приоритета:

- 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).

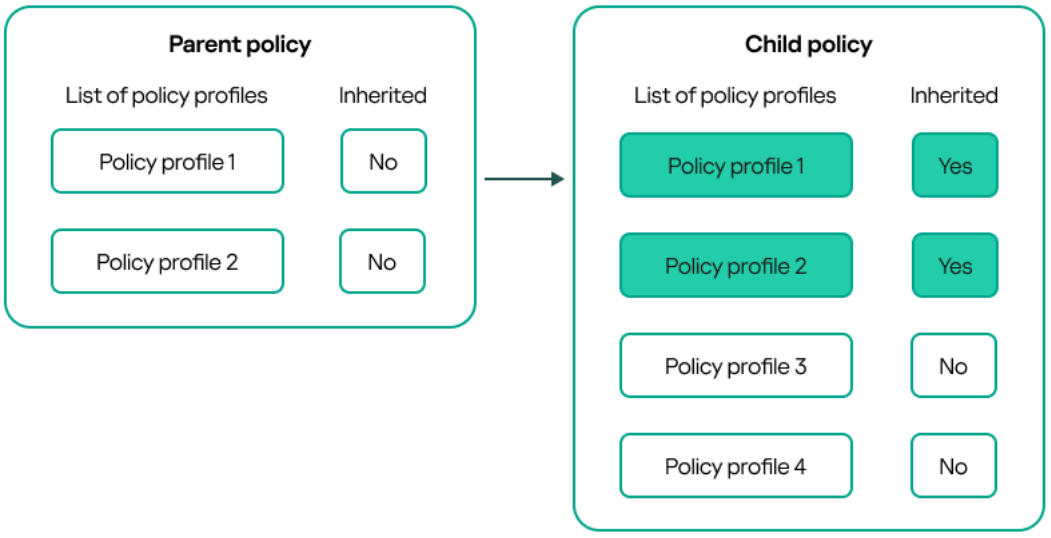


Конфигурация управляемого устройства соответствует условиям активации нескольких профилей политик

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 параметры реализованы на управляемом устройстве

Применения эффективных параметров на управляемом устройстве можно описать следующим образом:

- Значения всех незаблокированных параметров берутся из политики.
- Затем они перезаписываются значениями параметров управляемого приложения.
- Далее применяются заблокированные значения параметров из действующей политики. Значения заблокированных параметров изменяют значения разблокированных действующих параметров.

Управление политиками

В этом разделе описывается управление политиками и предоставляется информация о просмотре списка политик, создании политики, изменении политики, копировании политики, перемещении политики, принудительной синхронизации, просмотре диаграммы состояния распространения политики и удалении политики.

Просмотр списка политик

Вы можете просмотреть список политик, созданных на Сервере администрирования или в любой группе администрирования.

Чтобы просмотреть список политик:

1. В главном окне приложения перейдите в раздел **Управление активами** → **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. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

2. Выберите группу администрирования, для которой нужно создать политику:

   - Для корневой группы.

     В этом случае вы можете перейти к следующему шагу.

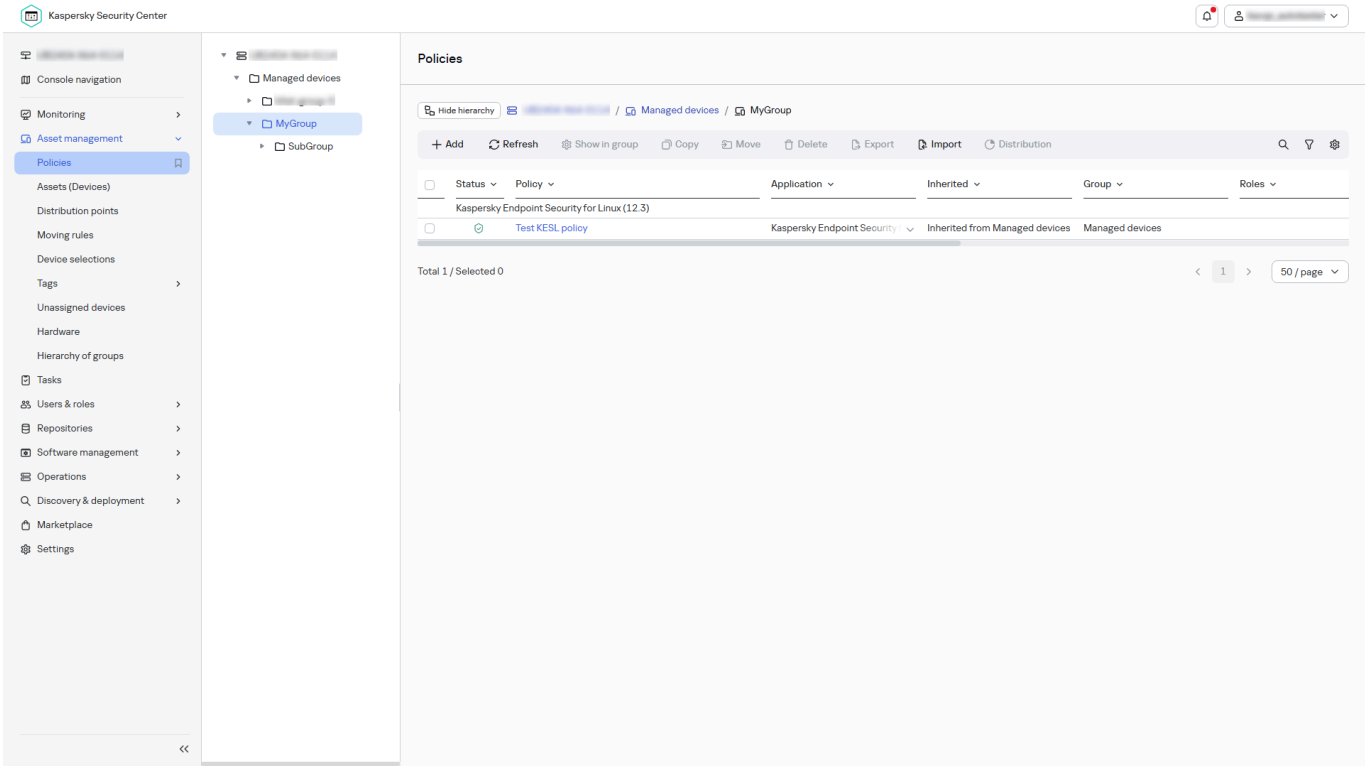
   - Для подгруппы:

     a. Нажмите на кнопку **Показать иерархию** в верхней части страницы.

        Название кнопки изменится на **Скрыть иерархию**.

     b. В открывшемся окне нажмите на название нужной подгруппы.

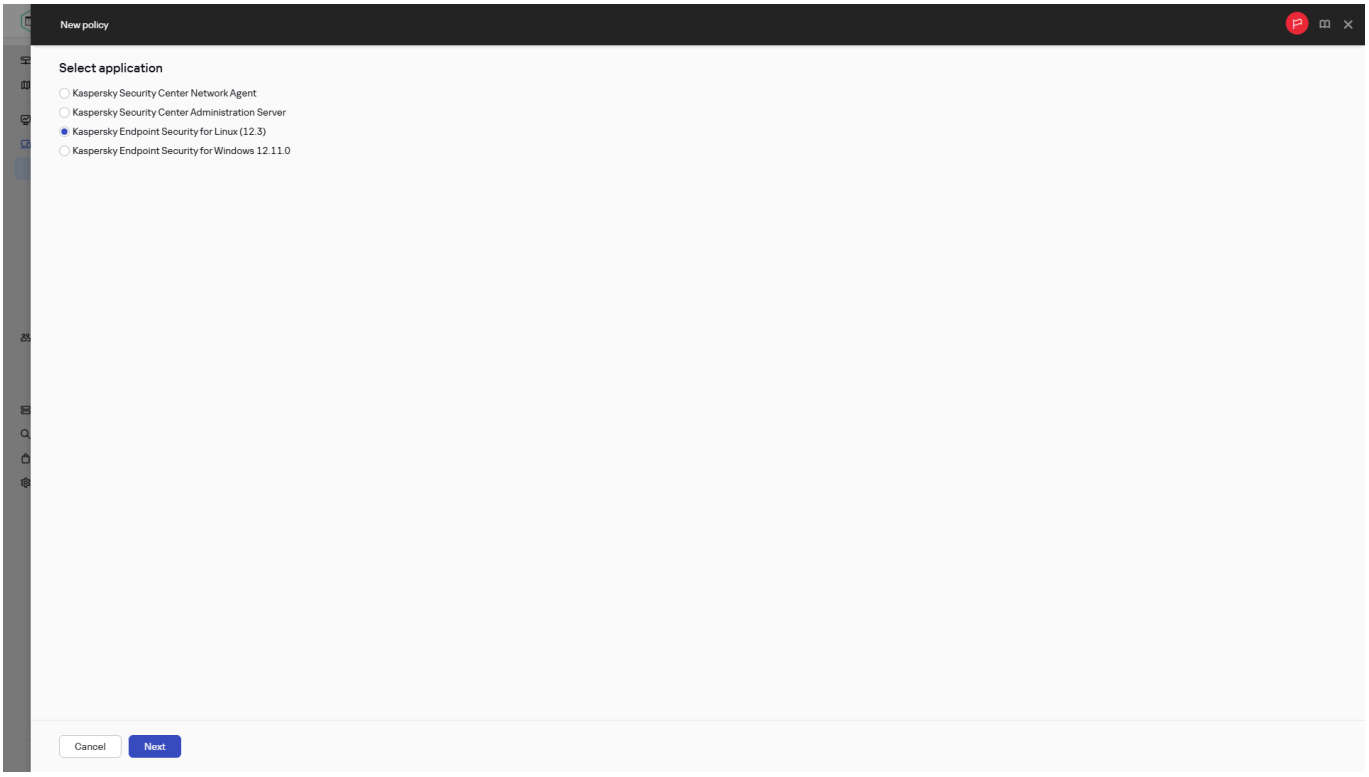
Путь к выбранной группе отображается в верхней части страницы. При необходимости вы можете нажать на ссылку с именем группы администрирования, чтобы перейти к группе. По умолчанию последняя ссылка в пути неактивна. Также вы можете закрыть окно иерархии, нажав на кнопку **Скрыть иерархию**.



Список политик

3. Нажмите на кнопку **Добавить**.

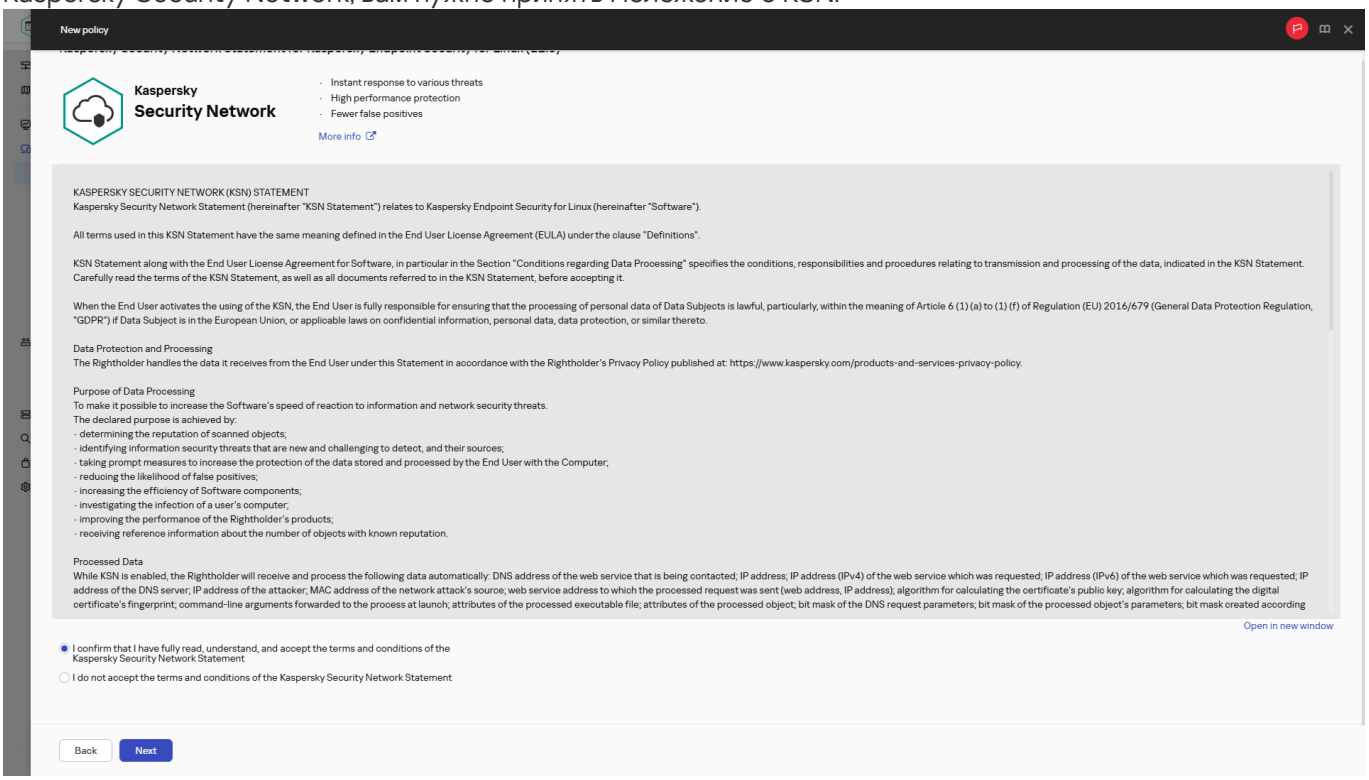
   Откроется окно **Выберите приложение**.



Создание политики

4. Выберите приложение, для которого требуется создать политику.

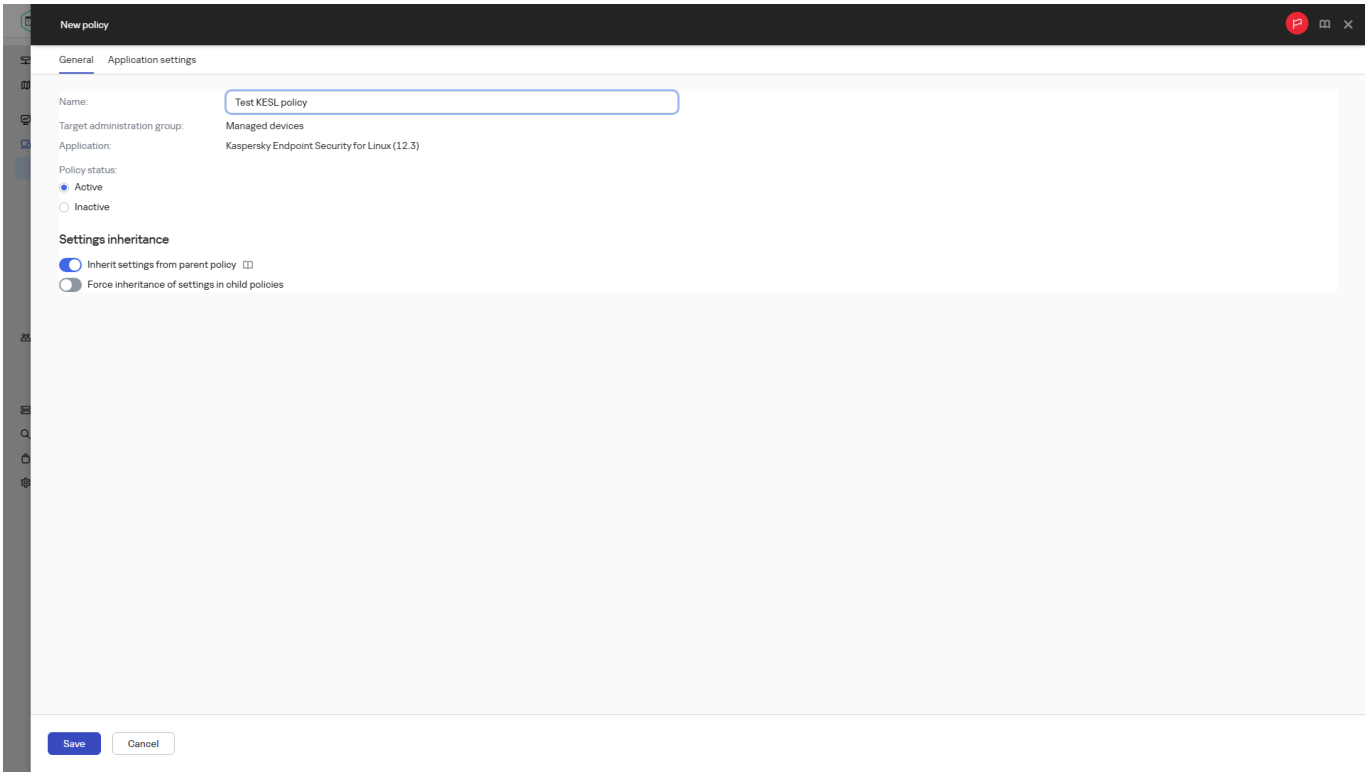
5. Если Kaspersky Security Network поддерживается приложением "Лаборатории Касперского", для которого вы создаете политику, вам будет предложено подтвердить Положение о KSN. Если вы хотите использовать Kaspersky Security Network, вам нужно принять Положение о KSN.



Принятие Положения о KSN

6. Нажмите на кнопку **Далее**.

Откроется окно параметров новой политики на вкладке **Общие**. При желании вы можете изменить следующие параметры политики, заданные по умолчанию: имя, состояние и наследование.



Окно параметров новой политики

7. Выберите вкладку **Параметры приложения**.

Или нажмите на кнопку **Сохранить**, чтобы выйти. Политика появится в списке политик, и вы сможете изменить ее свойства позже.

8. В левой области вкладки **Параметры приложения** выберите нужный вам раздел и в панели результатов измените параметры политики. Вы можете изменить параметры политики в каждом разделе.

   Набор параметров зависит от приложения, для которого вы создаете политику. Подробную информацию см. в следующих источниках:

   - Настройка Сервера администрирования
   - Параметры политики Агента администрирования
   - Справка Kaspersky Endpoint Security для Linux
   - Справка Kaspersky Endpoint Security для Windows

   Подробнее о параметрах других приложений безопасности см. в документации к соответствующему приложению.

   Чтобы отменить изменения, вы можете нажать на кнопку **Отмена**.

9. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения политики.

   Отображается уведомление со следующим сообщением: **Политика сохраняется и распространяется по иерархии Серверов администрирования**.

   Если политика проходит проверку, отображается следующее уведомление: **Политика сохранена**.

   Если политика не проходит проверку, отображается следующее уведомление: **Не удалось сохранить и распространить политику через иерархию Серверов администрирования. Обратитесь в Службу технической поддержки**. Вы можете проверить и изменить параметры политики, а затем повторить попытку. Если устранить проблему не удается, обратитесь в Службу технической поддержки.

В результате добавленная политика отображается в списке политик. После создания политики события изменения политик экспортируются в SIEM-систему, если этот параметр включен.

Общие параметры политик

Общие

На вкладке **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 вкладке **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на вкладках:

- **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 вкладке свойств Сервера администрирования (например, адрес получателя). Если вы хотите, измените эти параметры на вкладках **Электронная почта**, **SMS** и **Исполняемый файл для запуска**.

На вкладке **Настройка событий** отображаются уведомления при добавлении новых типов событий (например, в новой версии приложения), а также можно применить новые параметры, нажав на кнопку **Сохранить** или **Сохранить и закрыть**.

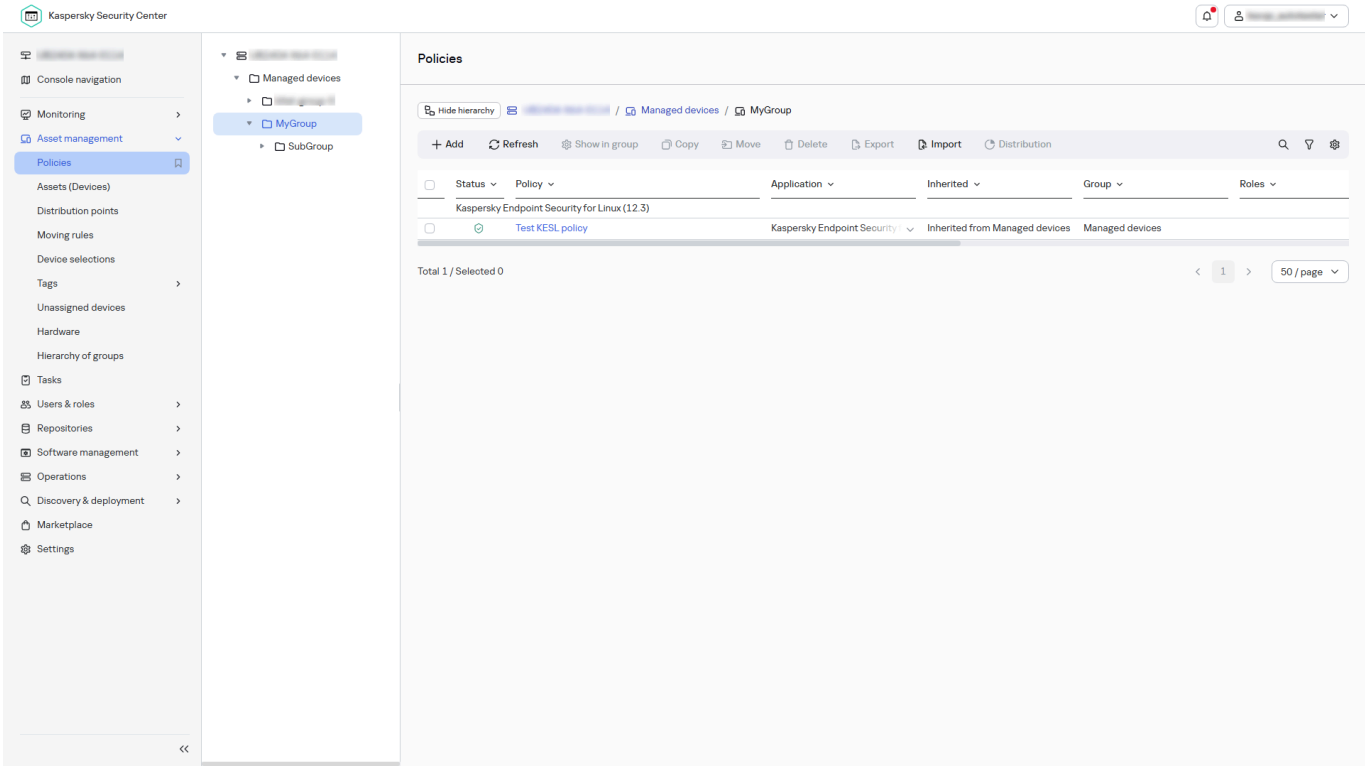
История ревизий

На вкладке **История ревизий** вы можете просмотреть список ревизий политики, сравнить ревизии политики, и при необходимости откатить изменения политики.

Изменение политики

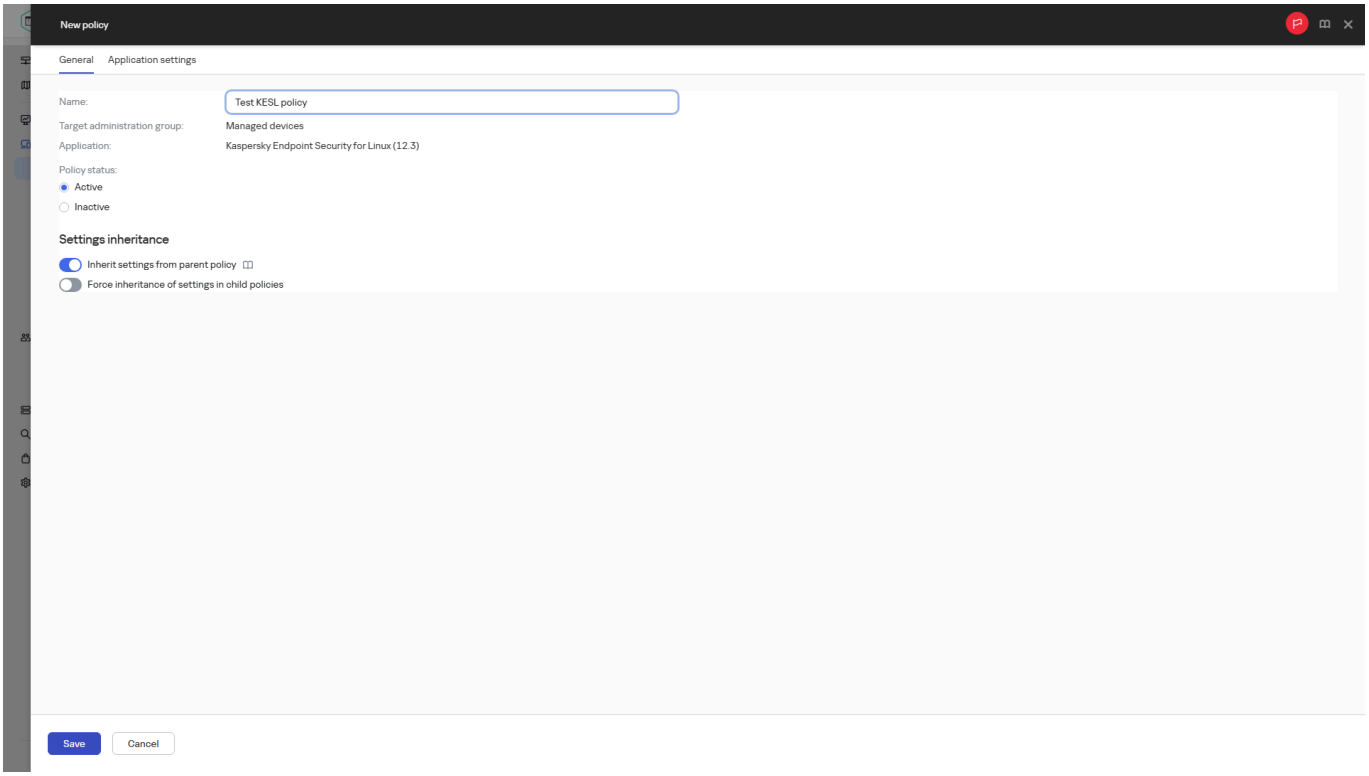
Чтобы изменить политику:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.



2. Выберите политику, которую требуется изменить.

Откроется окно свойств политики.



3. Укажите общие параметры и параметры приложения, для которого вы создаете политику. Подробную информацию см. в следующих источниках:

   - Настройка Сервера администрирования
   - Параметры политики Агента администрирования
   - Справка Kaspersky Endpoint Security для Linux
   - Справка Kaspersky Endpoint Security для Windows

   Подробнее о параметрах других приложений безопасности см. в документации к этим приложениям.

4. Нажмите на кнопку **Сохранить**.

   Отображается уведомление со следующим сообщением: **Политика сохраняется и распространяется по иерархии Серверов администрирования**.

   Если политика проходит проверку, отображается следующее уведомление: **Политика сохранена**.

   Если политика не проходит проверку, отображается следующее уведомление: **Не удалось сохранить и распространить политику через иерархию Серверов администрирования. Обратитесь в Службу технической поддержки**. Вы можете проверить и изменить параметры политики, а затем повторить попытку. Если устранить проблему не удается, обратитесь в Службу технической поддержки.

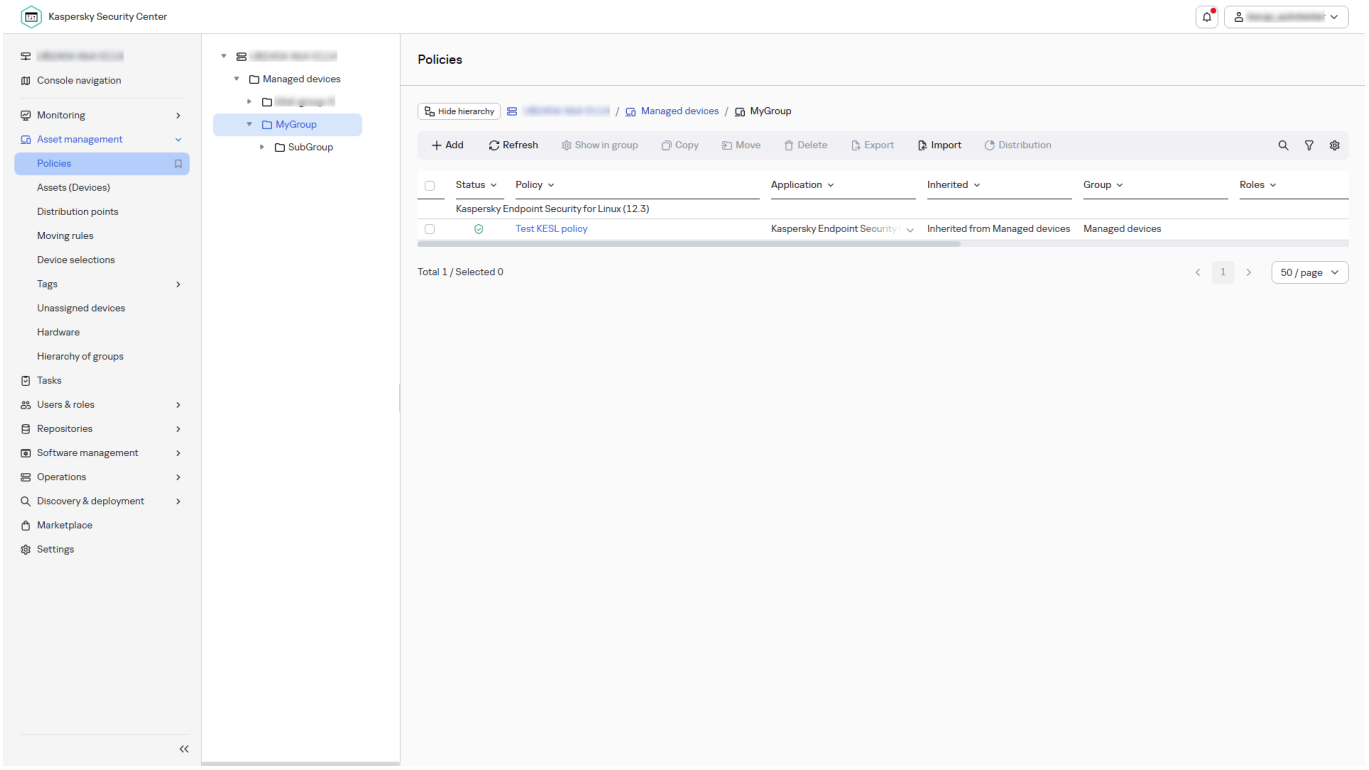
Изменения политики будут сохранены в свойствах политики и будут отображаться в разделе **История ревизий**. После изменения политики события изменения политик экспортируются в SIEM-систему, если этот параметр включен.

При необходимости вы можете сравнить ревизии политики. Параметр доступен для политик Сервера администрирования, Агента администрирования, Kaspersky Endpoint Security для Windows (начиная с версии веб-плагина 14.0) и Kaspersky Endpoint Security для Mac (начиная с версии веб-плагина 12.2.1 Patch A).

Включение и выключение параметра наследования политики

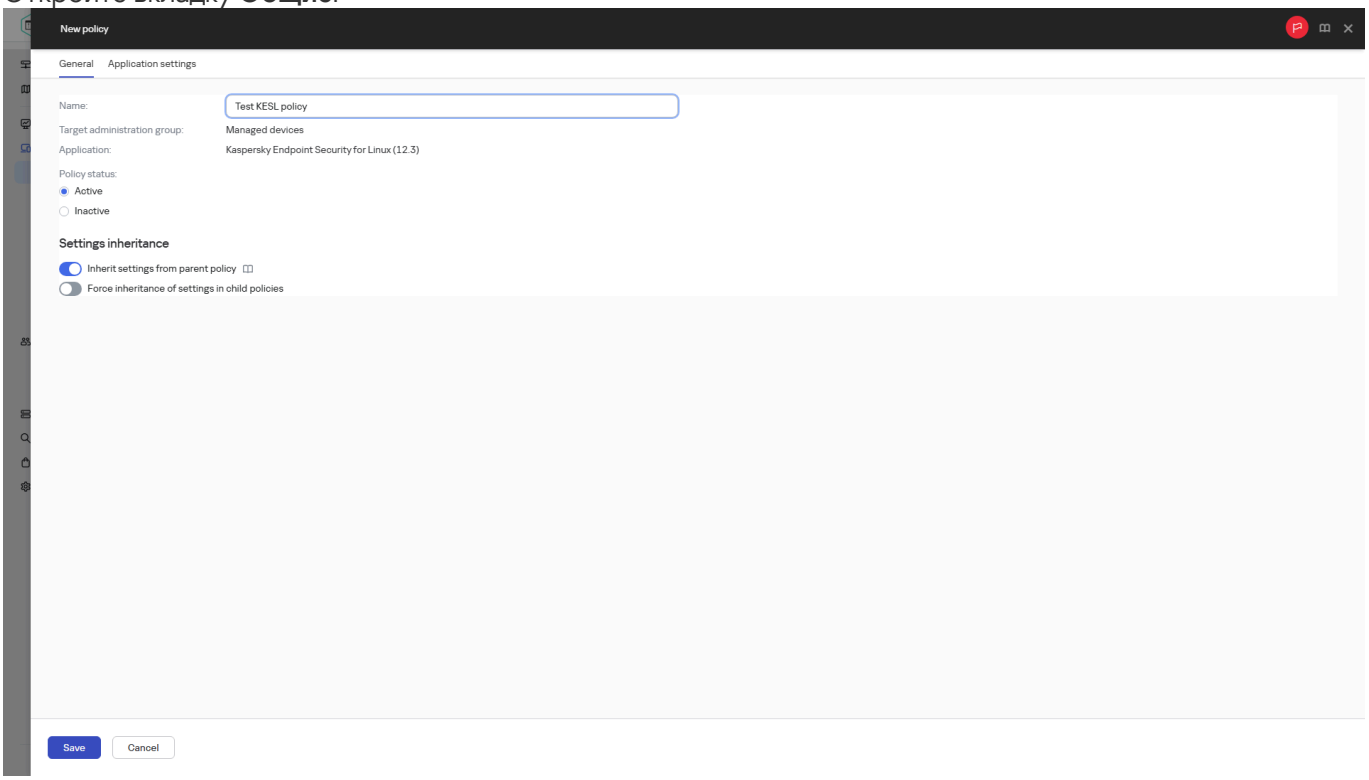
Чтобы включить или выключить параметр наследования в политике:

1. Откройте требуемую политику.



Список политик

2. Откройте вкладку **Общие**.



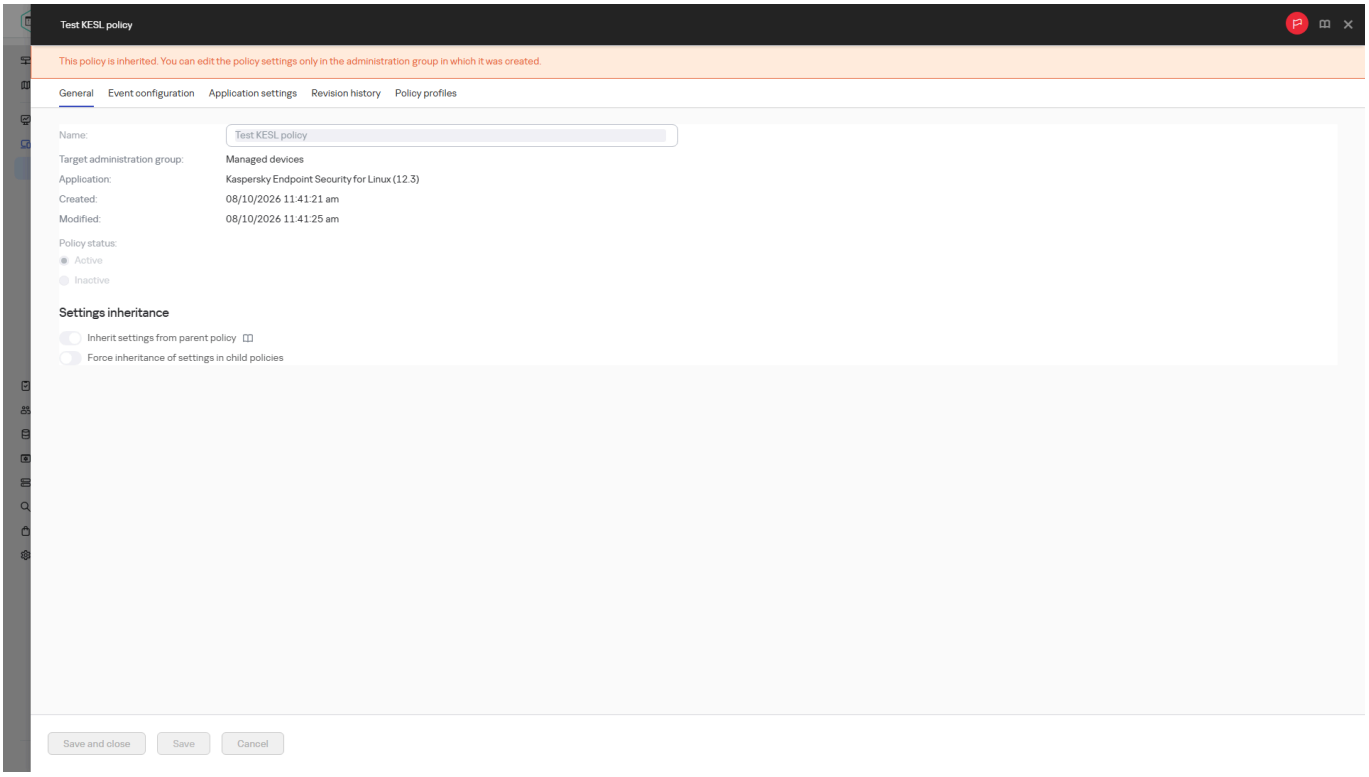
Создание политики

3. Включение или выключение наследования политики:

   - Если вы включили параметр **Наследовать параметры родительской политики** для дочерней группы и администратор заблокировал некоторые параметры в родительской политике, то вы не можете изменить эти параметры политики для дочерней политики.

   - Если вы выключили параметр **Наследовать параметры родительской политики** для дочерней политики, то 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**, это включит параметр **Наследовать параметры родительской политики** для каждой дочерней политики. В этом случае вы не можете выключить этот параметр для дочерних политик. Все параметры, которые заблокированы в родительской политике, принудительно наследуются в дочерних группах, и вы не можете изменить эти параметры в дочерних группах.



Заблокированные параметры политик

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.

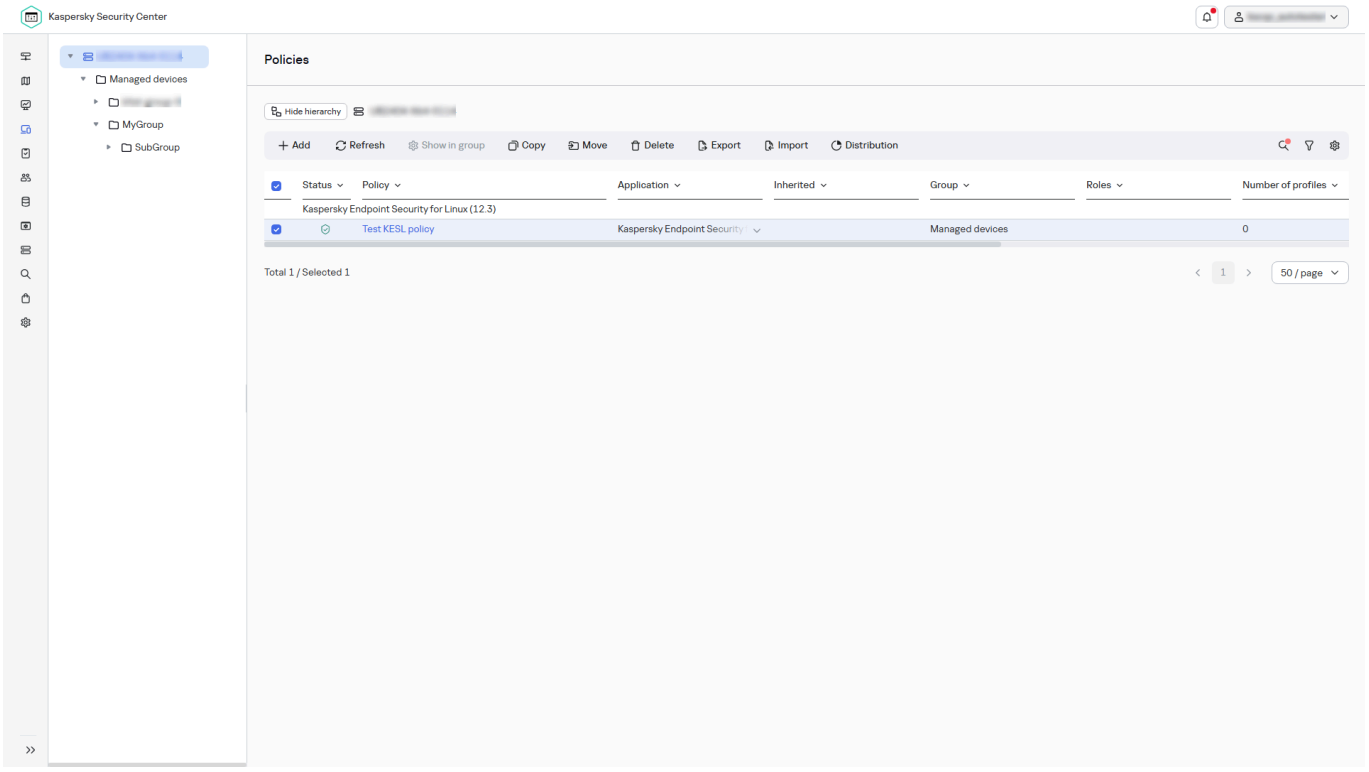
Копирование политики

Вы можете копировать политики из одной группы администрирования в другую.

Чтобы скопировать политику в другую группу администрирования:

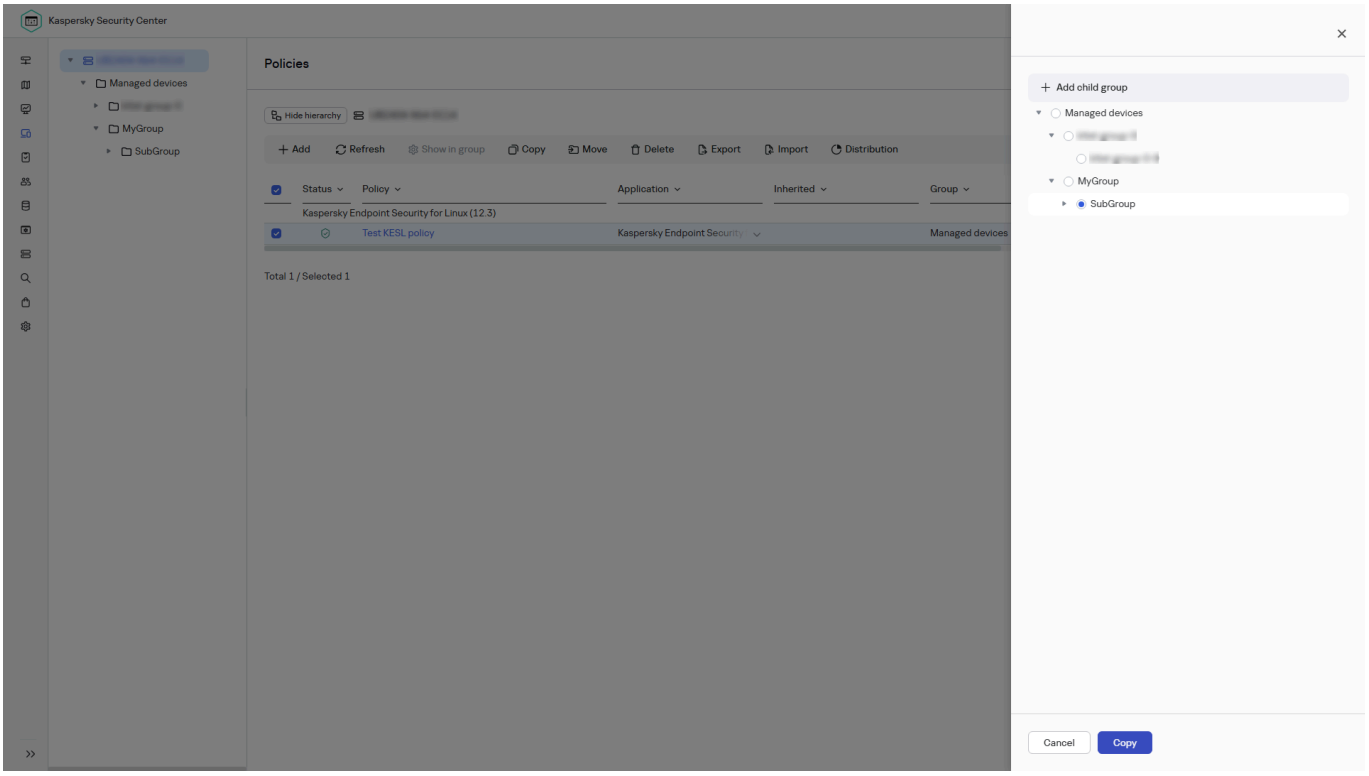
1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

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 **OK**, 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

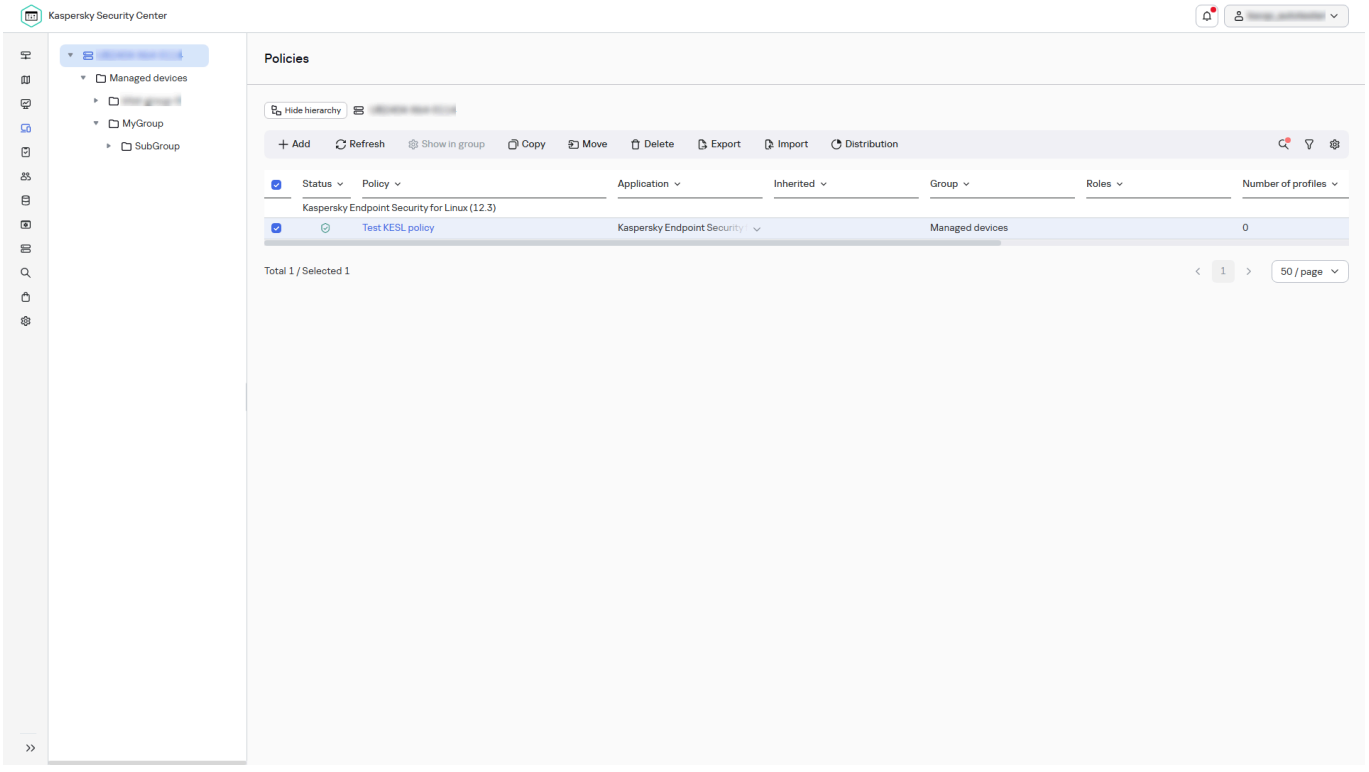
Вы можете перемещать политики из одной группы администрирования в другую. Например, вы хотите удалить одну группу администрирования, но использовать ее политики для другой группы администрирования. В этом случае вам может потребоваться, перед удалением старой группы администрирования, переместить политику из старой группы администрирования в новую.

> При перемещении политики в другую группу администрирования история изменений политики удаляется. На вкладке **История ревизий** отображается информация только о последних изменениях.

Чтобы переместить политику в другую группу администрирования:

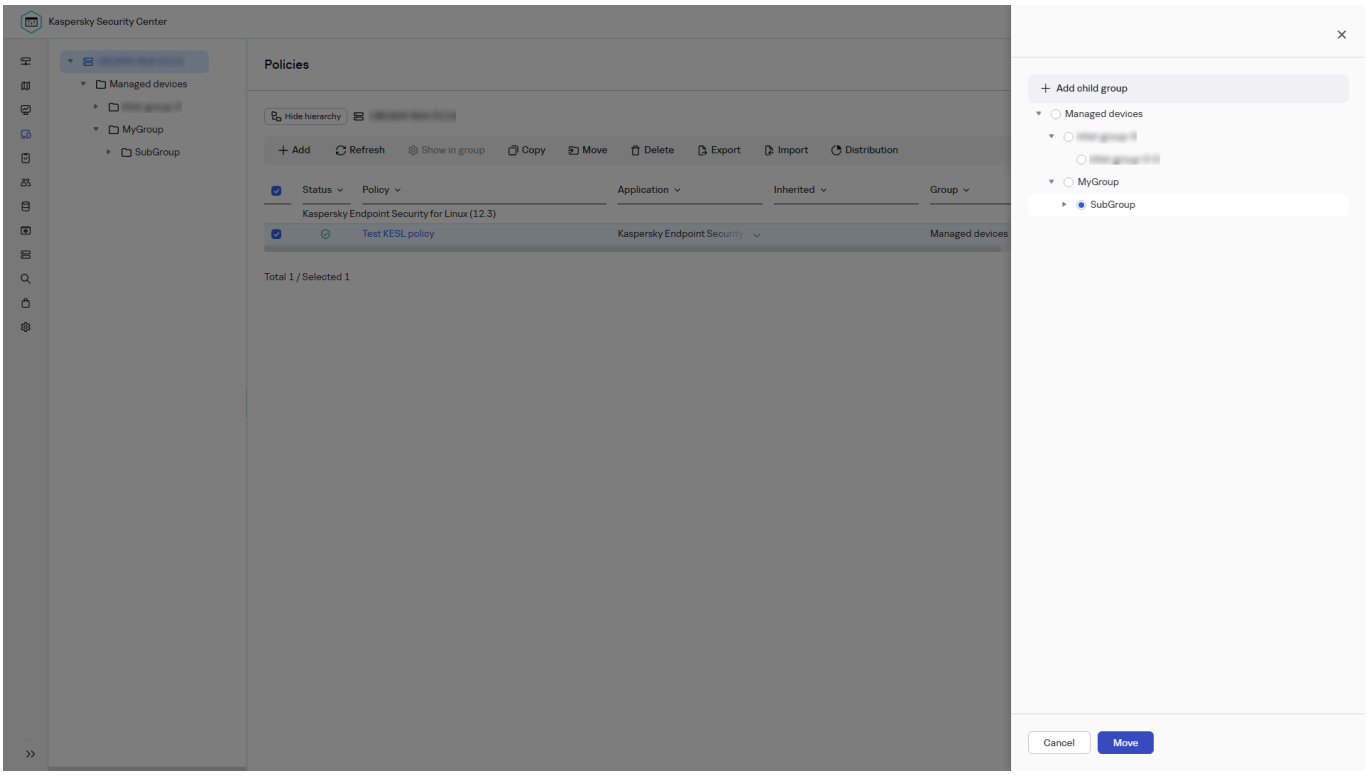
1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

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 **OK**, 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).

Экспорт политики

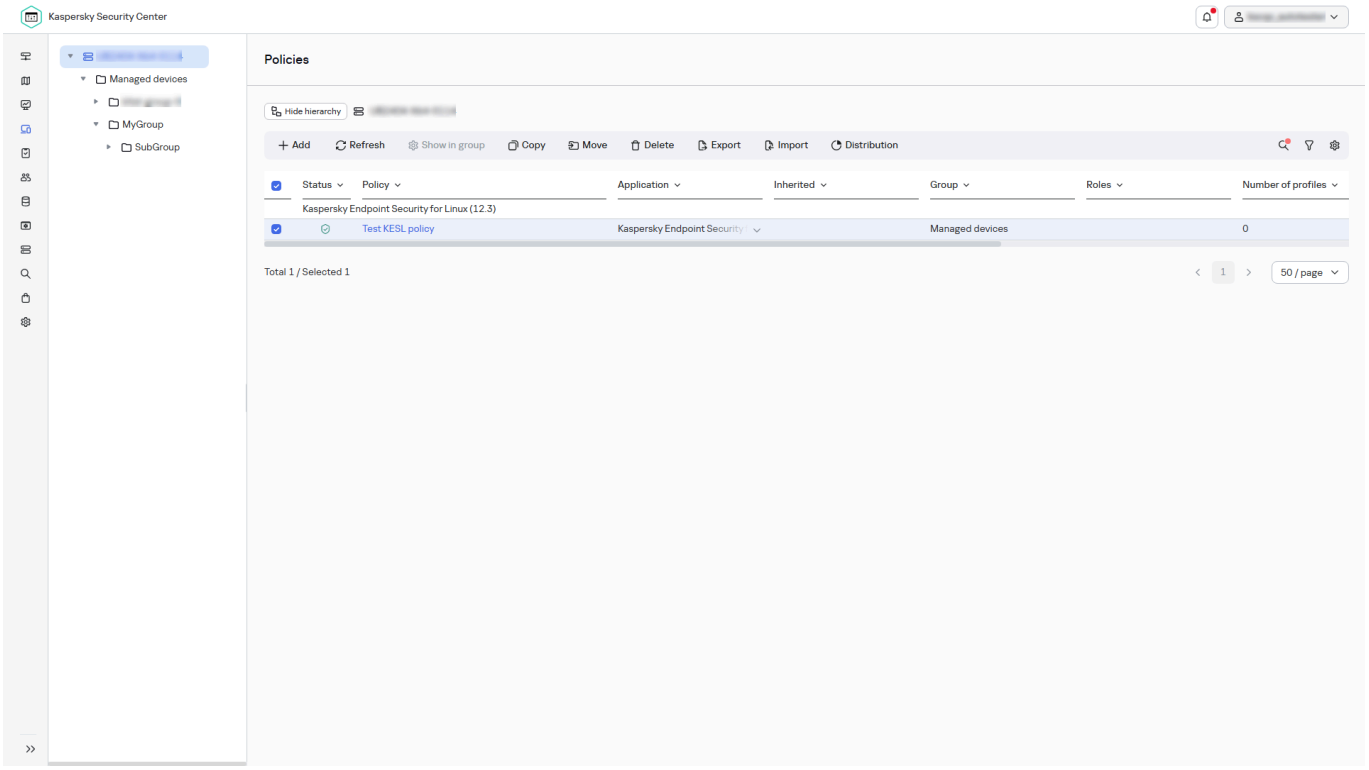
Kaspersky Security Center Linux позволяет сохранить политику, ее параметры и профили политики в файл KLP. Вы можете использовать файл KLP для импорта сохраненной политики как в Kaspersky Security Center Windows, так и в Kaspersky Security Center Linux.

Чтобы экспортировать политику:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

2. Установите флажок рядом с политикой, которую вы хотите экспортировать.

Невозможно экспортировать несколько политик одновременно. Если вы выберете более одной политики, кнопка **Экспортировать** будет неактивна.



Выбор политики для экспорта

3. Нажмите на кнопку **Экспортировать**.

4. В открывшемся окне **Сохранить как** укажите имя файла политики и путь. Нажмите на кнопку **Сохранить**.

   Окно **Сохранить как** отображается только в том случае, если вы используете Google Chrome, Microsoft Edge или Opera. Если вы используете другой браузер, файл политики автоматически сохраняется в папку **Загрузки**.

Импорт политики

Kaspersky Security Center Linux позволяет импортировать политику из файла KLP. Файл KLP содержит экспортированную политику, ее параметры и профили политики.

Чтобы импортировать политику:

1. В главном окне приложения перейдите в раздел **Управление активами → Политики**.

2. Нажмите на кнопку **Импортировать**.

3. Нажмите на кнопку **Обзор**, чтобы выбрать файл политики, который вы хотите импортировать.

4. В открывшемся окне укажите путь к файлу политики KLP и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл политики.

   Начнется обработка политики.

5. После успешной обработки политики выберите группу администрирования, к которой вы хотите применить политику.

6. Нажмите на кнопку **Завершить**, чтобы завершить импорт политики.

Появится уведомление с результатами импорта. Если политика успешно импортирована, вы можете перейти по ссылке **Подробнее** для просмотра свойств политики.

После успешного импорта политика отображается в списке политик. Также импортируются параметры и профили политики. Независимо от статуса политики, выбранной при экспорте, импортируемая политика неактивна. Вы можете изменить статус политики в свойствах политики.

Если параметры политики приложения содержат пароли, такую политику невозможно применить после импорта на другой Сервер Администрирования. В этом случае измените пароли в импортированной политике для ее применения.

Если имя новой импортированной политики идентично имени существующей политики, имя импортированной политики расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Принудительная синхронизация

Несмотря на то, что Kaspersky Security Center 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. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.
2. Выберите имя устройства, которое требуется синхронизировать с Сервером администрирования.

   В открывшемся окне свойств выберите раздел **Общие**.
3. Нажмите на кнопку **Синхронизировать сейчас**.

Приложение выполняет синхронизацию выбранного устройства с Сервером администрирования.

Синхронизация нескольких устройств

Чтобы осуществить принудительную синхронизацию между Сервером администрирования и несколькими управляемыми устройствами:

1. Откройте список устройств группы администрирования или выборку устройств:
   - Запустите выборку устройств, чтобы просмотреть список устройств.
   - В главном окне приложения перейдите в разделе **Управление активами** → **Управляемые устройства** и выберите группу администрирования, содержащую устройства для синхронизации:
     - Для корневой группы вы можете перейти к следующему шагу.
     - Для подгруппы в верхней части страницы нажмите на кнопку **Показать иерархию** и в открывшемся окне нажмите на имя подгруппы.

       Путь к выбранной группе отображается в верхней части страницы. При необходимости вы можете нажать на ссылку с именем группы администрирования, чтобы перейти к группе. По умолчанию последняя ссылка в пути неактивна. Также вы можете закрыть окно иерархии, нажав на кнопку **Скрыть иерархию**.
2. Установите флажки рядом с устройствами, которые требуется синхронизировать с Сервером администрирования.
3. Над списком управляемых устройств нажмите на кнопку с многоточием (...), а затем нажмите на кнопку **Синхронизировать сейчас**.

   Приложение выполняет синхронизацию выбранных устройств с Сервером администрирования.
4. В списке устройств проверьте, что время последнего подключения к Серверу администрирования для выбранных устройств изменилось на текущее время. Если время не изменилось, обновите содержимое страницы, нажав на кнопку **Обновить**.

Выбранные устройства синхронизированы с Сервером администрирования.

Просмотр времени доставки политики

После изменения политики для приложения "Лаборатории Касперского" на Сервере администрирования администратор может проверить, доставлена ли измененная политика на определенные управляемые устройства. Политика может быть доставлена во время регулярной или принудительной синхронизации.

Чтобы просмотреть дату и время доставки политики приложения на управляемые устройства:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.
2. Выберите имя устройства, которое требуется синхронизировать с Сервером администрирования.

   В открывшемся окне свойств выберите раздел **Общие**.
3. Перейдите на вкладку **Приложения**.

4. Выберите приложение, для которого требуется посмотреть дату синхронизации политики.

   Откроется окно политики приложения, с выбранным разделом **Общие**, и отобразится дата и время доставки политики.

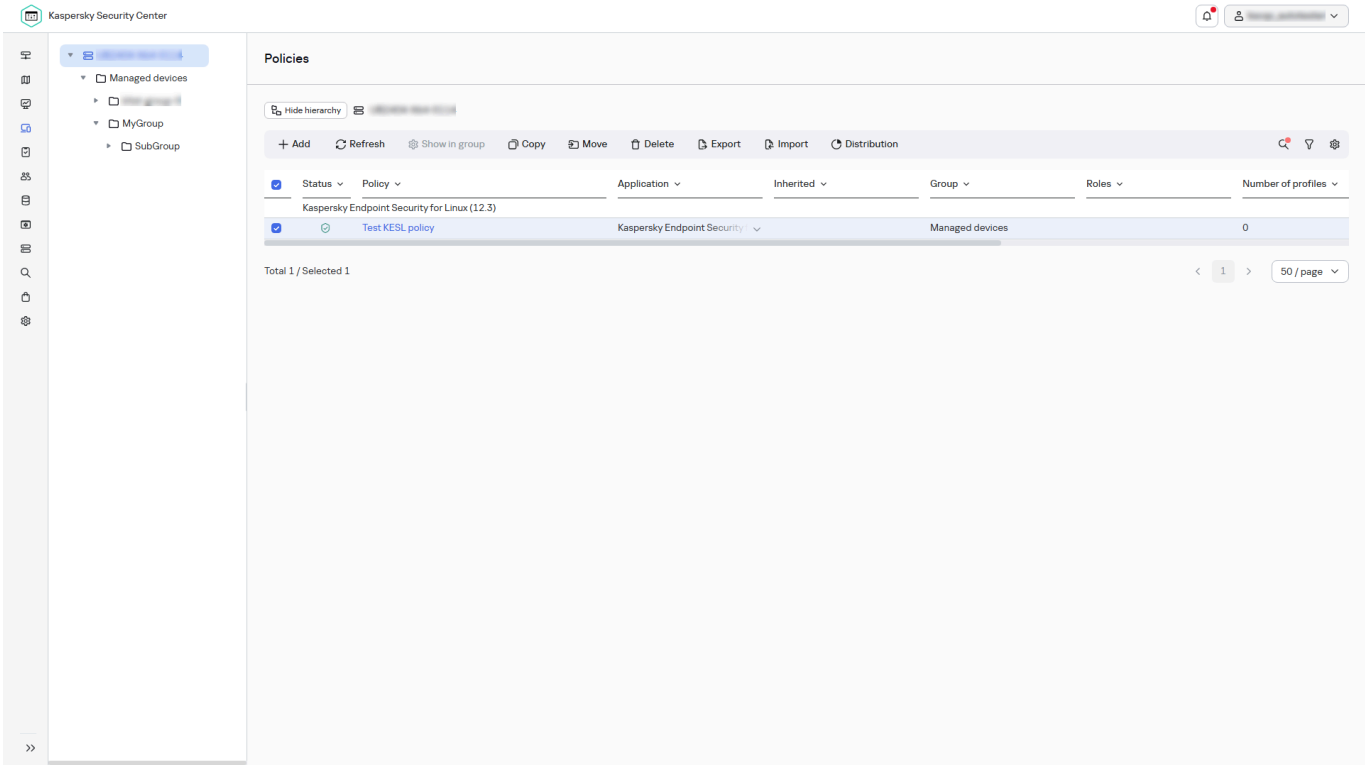
Просмотр диаграммы состояния применения политики

В Kaspersky Security Center Linux вы можете просматривать состояние применения политики на каждом устройстве на диаграмме.

Чтобы просмотреть статус применения политики на каждом устройстве:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

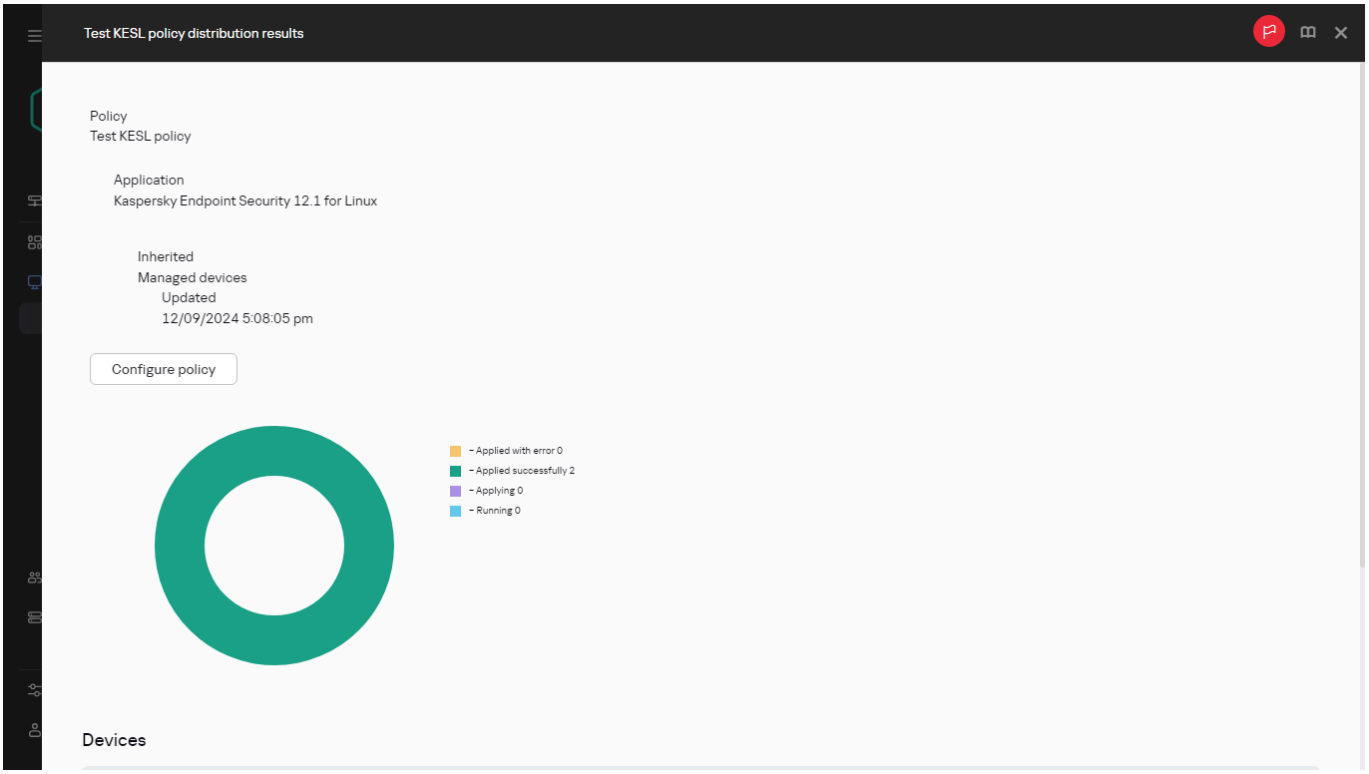
2. Установите флажок рядом с именем политики, для которой вы хотите просмотреть состояние применения на устройстве.



Список политик

3. В появившемся меню выберите ссылку **Результаты применения**.

Откроется окно **Результат распространения <название политики>**.



Результаты распространения политики

4. В открывшемся окне **Результат распространения <название политики>** отображается **Описание статуса**.

Вы можете изменить количество результатов, отображаемых в списке результатов применения политики. Максимальное количество устройств равно 100 000.

Чтобы изменить количество устройств, отображаемых в списке с результатами применения политики:

1. В главном окне приложения перейдите в раздел **Параметры → Параметры интерфейса**.
2. В поле **Максимальное количество устройств, отображаемых в результатах распространения политики** введите количество устройств (до 100 000).

   По умолчанию количество устройств равно 5000.
3. Нажмите на кнопку **Сохранить**.

   Параметры сохранены и применены.

Автоматическая активация политики по событию "Вирусная атака"

Чтобы политика активировалась автоматически при наступлении события "Вирусная атака":

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.
2. Выберите раздел **Вирусная атака**.
3. В правой панели нажмите на ссылку **Настроить активацию политик по возникновению события "Вирусная атака"**.

   Откроется окно **Активация политик**.

4. В разделе, к которому относится компонент обнаруживший вирусную атаку (антивирусы для рабочих станций и файловых серверов, антивирусы для почтовых серверов, антивирусы защиты периметра), выберите нужную вам запись и затем нажмите на кнопку **Добавить**.

   Откроется окно с группой администрирования **Управляемые устройства**.

5. Нажмите на значок шеврона (>) рядом с **Управляемые устройства**.

   Отобразится иерархия групп администрирования и их политик.

6. В иерархии групп администрирования и их политик нажмите на название политики (или политик), которая активируется при возникновении вирусной атаки.

   Чтобы выбрать все политики в списке или в группе, установите флажок рядом с требуемым именем.

7. Нажмите на кнопку **Сохранить**.

   Окно с иерархией групп администрирования и их политиками закрыто.

Выбранные политики добавляются в список политик, которые активируются при возникновении вирусной атаки. Выбранные политики активируются во время вирусной атаки независимо от того, активны они или неактивны.

В случае активации политики по событию Вирусная атака вернуться к предыдущей политике можно только вручную.

Удаление политики

Вы можете удалить политику, если она больше не нужна. Вы можете удалить только неунаследованную политику в выбранной группе администрирования. Если политика унаследована, вы можете удалить ее только в группе администрирования, в которой она была создана.

Чтобы удалить политику:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

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. После удаления политики события изменения политик экспортируются в SIEM-систему, если этот параметр включен.

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, удалении, экспорте и импорте профиля политики.

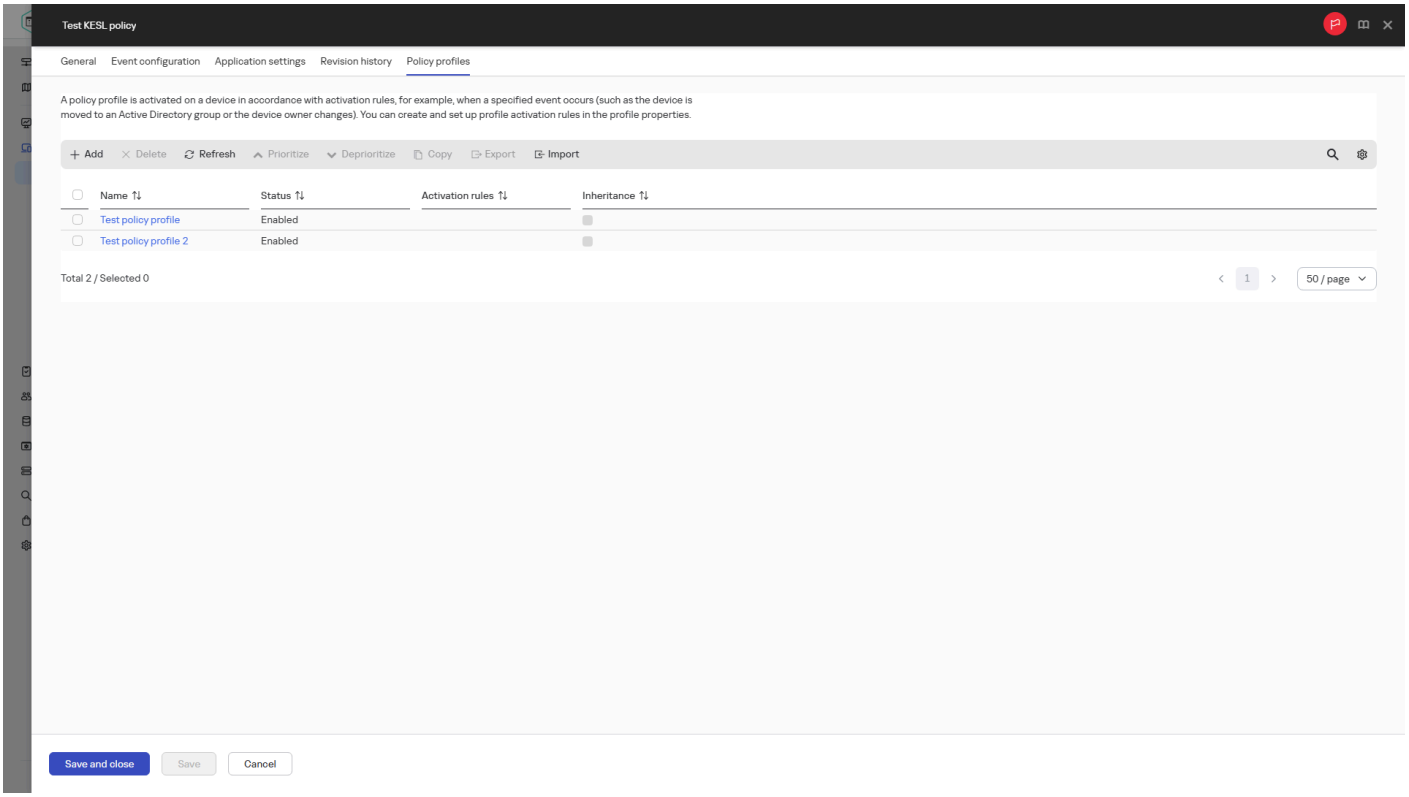
Просмотр профилей политики

Чтобы просмотреть профили политики:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Выберите политику, профили которой требуется просмотреть.

   Откроется окно свойств политики на вкладке **Общие**.
3. Откройте вкладку **Профили политики**.

Профили политики отобразятся в виде таблицы. Если у политики нет профилей политики, отобразится пустая таблица.



Список профилей политики

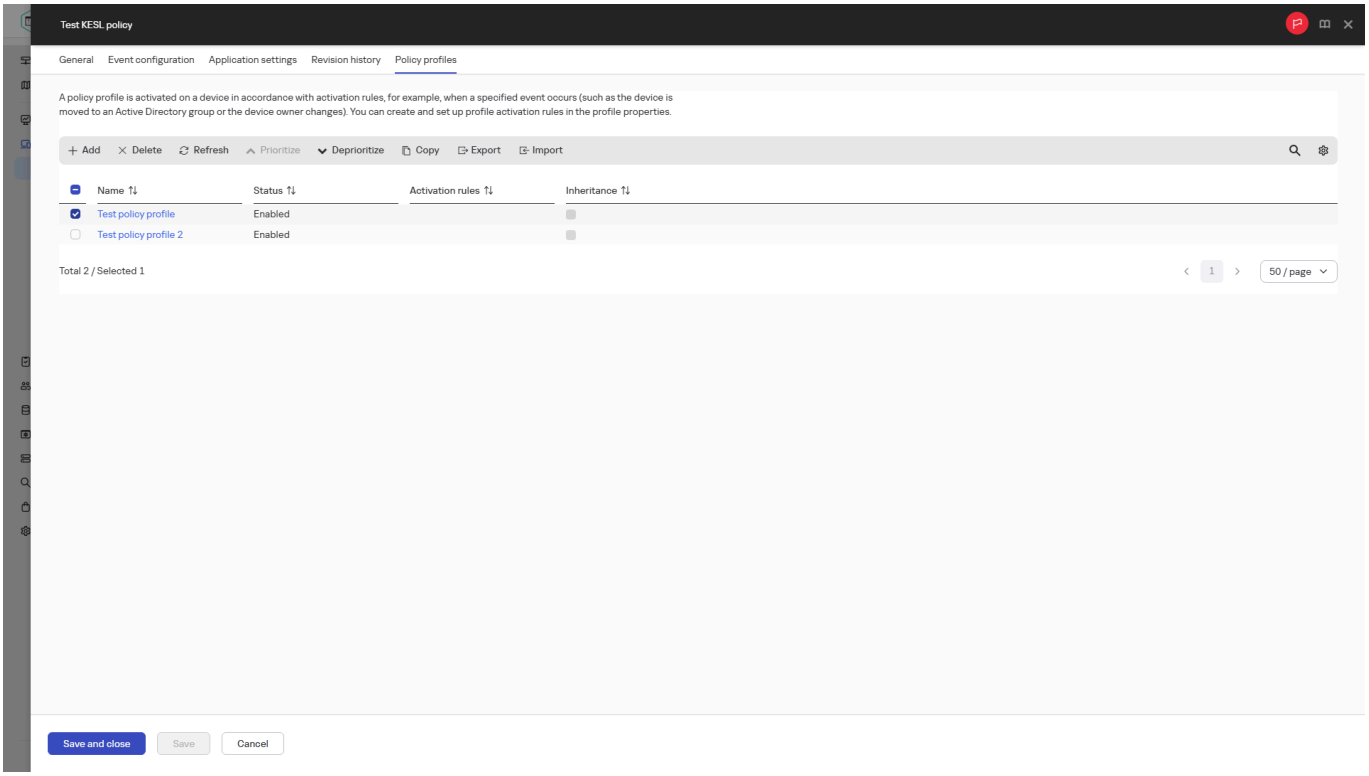
Изменение приоритета профиля политики

Чтобы изменить приоритет профиля политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.
2. На вкладке **Профили политики** установите флажок рядом с профилем политики, для которого требуется изменить приоритет.
3. Установите профиль политики на новую позицию в списке с помощью кнопок **Повысить приоритет** или **Понизить приоритет**.

Чем выше расположен профиль политики в списке, тем выше его приоритет.



4. Нажмите на кнопку **Сохранить**.

Приоритет выбранного профиля политики изменен и применен.

Создание профиля политики

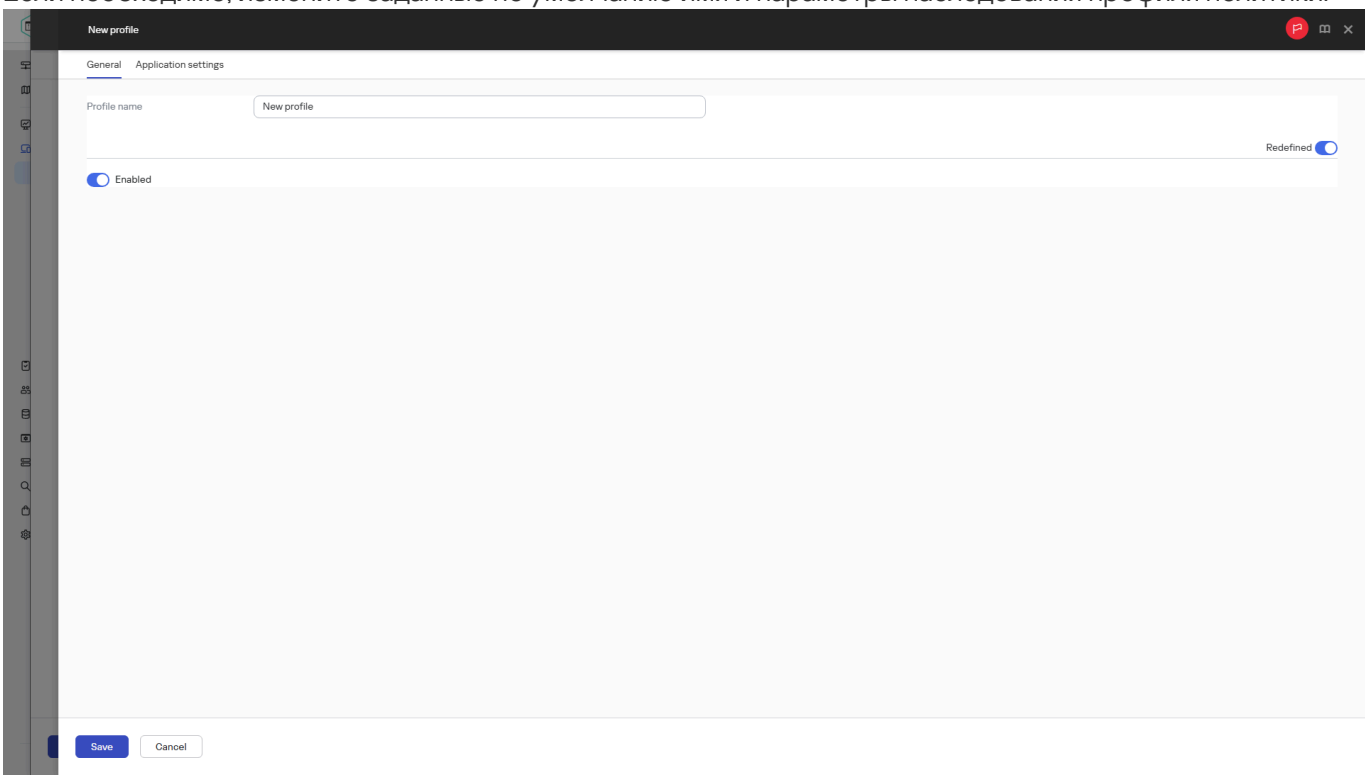
Чтобы создать профиль политики:

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.



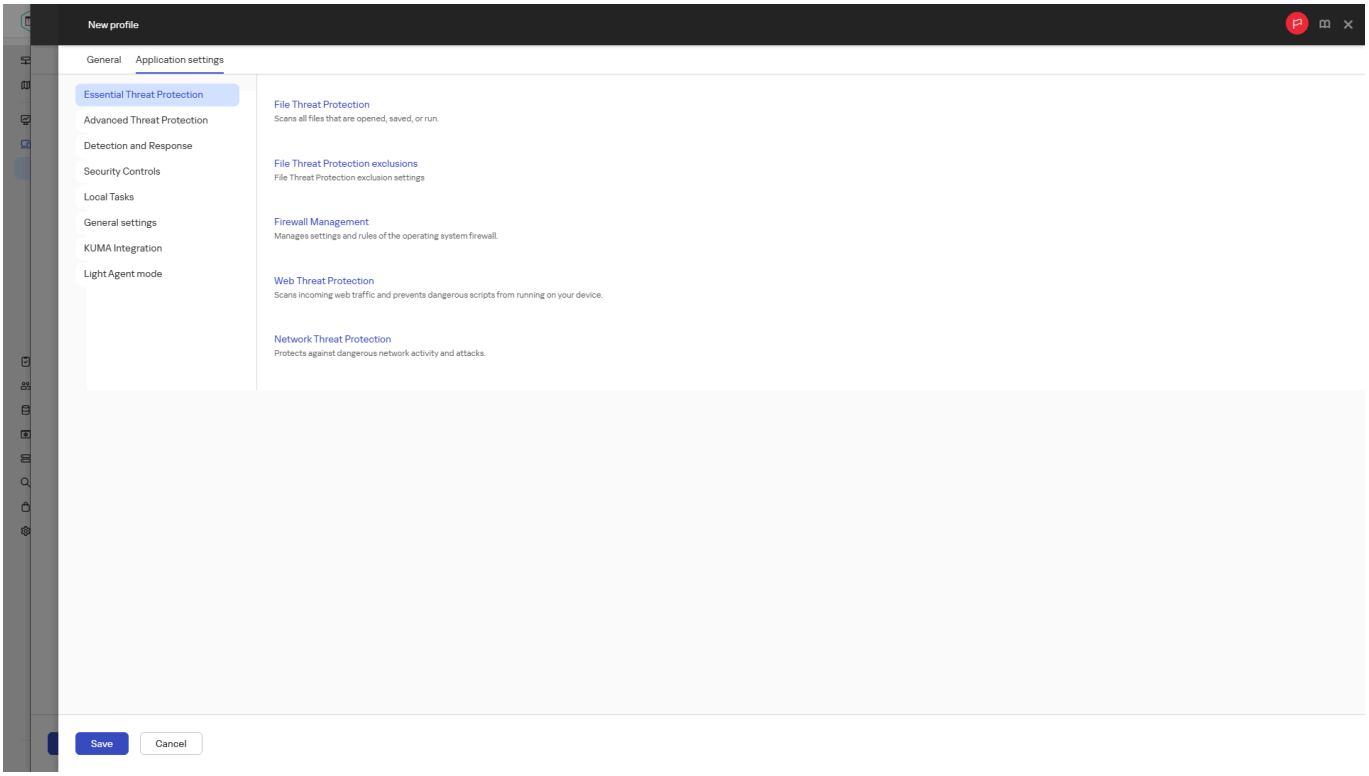
Создание профиля политики

4. Выберите вкладку **Параметры приложения**.

   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 вкладки **Параметры приложения** выберите нужный вам раздел и в панели результатов измените параметры профиля политики. Вы можете изменить параметры профиля политики в каждом разделе.

Чтобы отменить изменения, вы можете нажать на кнопку **Отмена**.



Указание параметров профиля политики

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 вкладке **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

Чтобы создать правило активации профиля политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. На вкладке **Профили политики** нажмите на профиль политики, для которого требуется создать правило активации.

   Если список профилей политики пуст, вы можете создать профиль политики.

3. На вкладке **Правила активации** нажмите на кнопку **Добавить**.

   Откроется окно с правилами активации профиля политики.

4. Укажите имя правила активации.

5. Установите флажки напротив условий, которые должны влиять на активацию создаваемого профиля политики:

   Общие правила активации профиля политики

   Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от состояния автономного режима устройства, правила подключения устройства к Серверу администрирования и назначенных устройству тегов.

   Для этого параметра на следующем шаге укажите:

   Статус устройства

   Определяет условие присутствия устройства в сети:

   - **В сети** – устройство находится в сети, Сервер администрирования доступен.
   - **Не в сети** – устройство находится во внешней сети, то есть Сервер администрирования недоступен.
   - **Неизвестно** – критерий не применяется.

   Параметры сетевого местоположения устройства

   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 профиля политики на устройстве в зависимости от объема памяти и количества логических процессоров устройства.

  Для этого параметра на следующем шаге укажите:

  Объем оперативной памяти (МБ)

  Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по объему оперативной памяти устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

  - объем оперативной памяти устройства меньше указанного значения (знак "<");
  - объем оперативной памяти устройства больше указанного значения (знак ">").

  Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать объем оперативной памяти устройства. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

  Количество логических процессоров

  Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по количеству логических процессоров устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

  - количество логических процессоров устройства меньше или равно указанному значению (знак "<");
  - количество логических процессоров устройства больше или равно указанному значению (знак ">").

Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать количество логических процессоров устройства. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- **Правила для назначения роли**

  Для этого параметра на следующем шаге укажите:

  Активировать профиль политики по наличию роли у владельца устройства

  Включите этот параметр, чтобы настроить и включить правило активации профиля политики на устройстве в зависимости от наличия определенной роли у его владельца. Добавить роль вручную из списка существующих ролей.

  Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием.

- **Правила для использования тега**

  Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от тегов, назначенных устройству. Вы можете активировать профиль политики либо на устройствах, которые имеют выбранные теги, либо не имеют их.

  Для этого параметра на следующем шаге укажите:

  Список тегов

  В списке тегов задайте правило включения устройств в профиль политики, установив флажки нужным тегам.

  Вы можете добавить в список новые теги, введя их в поле над списком и нажав на кнопку **Добавить**.

  В профиль политики будут включены устройства, в описании которых есть все выбранные теги. Если флажки сняты, критерий не применяется. По умолчанию флажки сняты.

  Применить к устройствам без выбранных тегов

  Включите параметр, если необходимо инвертировать выбор тегов.

  Если параметр включен, в профиль политики будут включены устройства, в описании которых нет выбранных тегов. Если этот параметр выключен, критерий не применяется.

  По умолчанию параметр выключен.

- **Правила для использования Active Directory**

  Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от размещения устройства в подразделении Active Directory или же от членства устройства или его владельца в группе безопасности Active Directory.

  Для этого параметра на следующем шаге укажите:

  Членство владельца устройства в группе безопасности Active Directory

  Если параметр включен, профиль политики активируется на устройстве, владелец которого является членом указанной группы безопасности. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

  Членство устройства в группе безопасности Active Directory

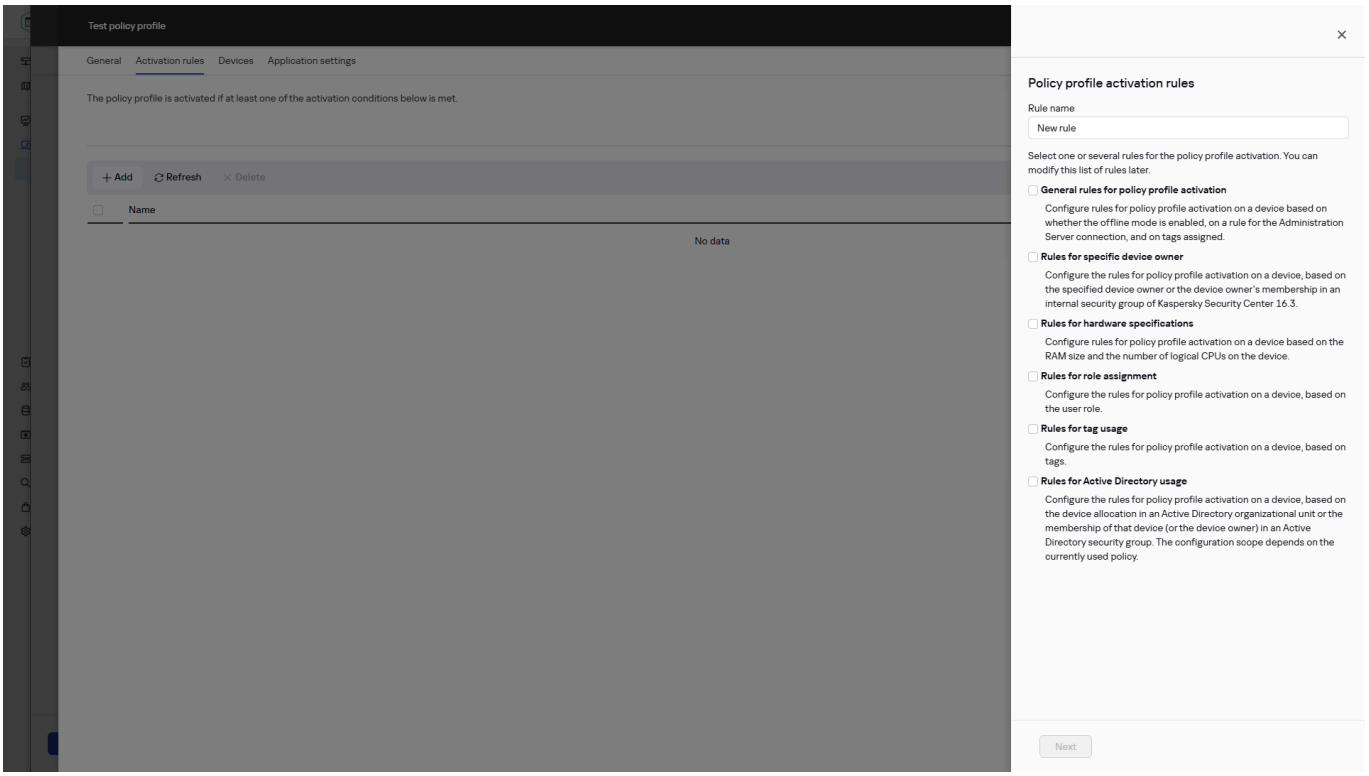
  Если параметр включен, профиль политики активируется на устройстве. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

  Размещение устройства в подразделении Active Directory

Если параметр включен, профиль политики активируется на устройстве, которое входит в указанное подразделение Active Directory (OU). Если параметр выключен, критерий активации профиля не применяется.

По умолчанию параметр выключен.

От выбора параметров на этом шаге зависит дальнейшее количество окон мастера. Вы можете изменить правила активации профиля политики позже.



Создание правила активации профиля политики.

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 вкладке **Правила активации**. Вы можете изменить или удалить правило активации профиля политики.

Несколько правил активации могут выполняться одновременно.

Удаление профиля политики

Чтобы удалить профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. На странице **Профили политики** установите флажок рядом с профилем политики, который вы хотите удалить, и нажмите на кнопку **Удалить**.

3. В появившемся окне нажмите на кнопку **Удалить** еще раз.

Профиль политики удален. Если политика наследуется группой более низкого уровня, профиль политики остается в этой группе, но становится профилем политики этой группы. Это позволяет уменьшить изменения в параметрах управляемых приложений, установленных на устройствах групп нижнего уровня.

Экспорт и импорт профиля политики

Вы можете сохранить профиль политики в файл KLPROF без экспорта политики, а затем использовать этот файл KLPROF для импорта сохраненного профиля в политику.

Это позволяет быстро восстановить параметры профиля политики вместо их повторной настройки.

Профиль политики импортируется в политику той же версии приложения, из которой вы экспортировали профиль. Для приложений, поддерживающих обратную совместимость политик (например, Kaspersky Endpoint Security для Windows), вы можете импортировать профили политики в разные версии политики.

Чтобы экспортировать профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. На вкладке **Профили политики** нажмите на профиль политики, который вы хотите экспортировать.

3. В панели инструментов нажмите на кнопку **Экспортировать**.

4. В открывшемся окне укажите директорию, в которую вы хотите сохранить в файл с профилем политики.

   При необходимости измените имя файла.

5. Нажмите на кнопку **Сохранить**.

Если операция завершена успешно, на экране отобразится соответствующее сообщение. Иначе отобразится сообщение об ошибке.

Чтобы импортировать профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. В панели инструментов нажмите на кнопку **Импортировать**.

3. В открывшемся окне выберите файл KLPROF с нужным профилем политики и нажмите на кнопку **Открыть**.

   Максимальный размер импортируемого файла – 4 МБ.

Если операция завершена успешно, на экране отобразится соответствующее сообщение. Иначе отобразится сообщение об ошибке.

Профиль политики импортируется с именем, которое он имел при экспорте, а не с именем файла KLPROF.
Файл импортируется со статусом **Выключен** и самым низким приоритетом, независимо от приоритета, который был у профиля политики перед экспортом.

Вы не можете выполнить импорт в следующих случаях:

- У политики уже есть профиль с таким же именем.
- Количество профилей в политике равно 100.

Параметры политики Агента администрирования

Чтобы настроить параметры политики Агента администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на название политики Агента администрирования.

   Откроется окно свойств политики Агента администрирования. Окно свойств содержит вкладки и параметры, описанные ниже.

См. таблицу сравнения, в которой подробно описано применение параметров, описанных ниже, в зависимости от используемой операционной системы.

Общие

На этой вкладке можно изменить название политики, состояние политики и настроить наследование параметров политики:

- В поле **Имя** вы можете изменить название 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.

  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 этой вкладке можно настроить регистрацию событий и оповещение о событиях. События распределяются по уровням важности в следующих разделах:

- **Отказ функционирования**
- **Предупреждение**
- **Информационное сообщение**

В каждом разделе в списке событий отображаются названия событий и срок хранения событий на Сервере администрирования по умолчанию (в днях). После того как вы нажмете на тип события, можно настроить параметры регистрации и уведомления о событиях, выбранных в списке. По умолчанию общие настройки уведомлений, указанные для всего Сервера администрирования, используются для всех типов событий. Однако можно изменить определенные параметры для заданных типов событий.

Например, в разделе **Предупреждение**, вы можете настроить тип события **Произошла проблема безопасности**. Такие события могут произойти, например, когда свободное место на диске точки распространения меньше 2 ГБ (для установки приложений и удаленной загрузки обновлений требуется не менее 4 ГБ). Чтобы настроить событие **Произошла проблема безопасности**, нажмите на него и укажите, где хранить произошедшие события и как о них уведомлять.

Если Агент администрирования обнаруживает проблему безопасности, вы можете управлять этой проблемой безопасности с помощью параметров управляемого устройства.

Параметры

В разделе **Параметры** можно настроить параметры политики Агента администрирования:

Распространять файлы только через точки распространения

Если этот параметр включен, Агенты администрирования на управляемых устройствах получают обновления только от точек распространения.

Если этот параметр выключен, Агенты администрирования на управляемых устройствах получают обновления от точек распространения или от Сервера администрирования.

> Обратите внимание, что приложения безопасности на управляемых устройствах получают обновления от источника, заданного в задаче обновления для каждого приложения безопасности. Если вы включили параметр **Распространять файлы только через точки распространения**, убедитесь, что Kaspersky Security Center Linux установлен в качестве источника обновлений в задачах обновления.

По умолчанию параметр выключен.

Максимальный размер очереди событий (МБ)

В поле можно указать максимальное место на диске, которое может занимать очередь событий.

По умолчанию указано значение 2 МБ.

Приложение может получать расширенные данные политики на устройстве

Агент администрирования, установленный на управляемом устройстве, передает информацию о применяемой политике в приложение безопасности (например, Kaspersky Endpoint Security для Linux). Передаваемая информация отображается в интерфейсе приложения безопасности.

Агент администрирования передает следующую информацию:

- время доставки политики на управляемое устройство;
- имя активной политики в момент доставки политики на управляемое устройство;
- название политики для автономных пользователей в момент доставки политики на управляемое устройство (недоступно для Агента администрирования для Linux);
- имя и полный путь группы администрирования, которой принадлежит управляемое устройство на момент доставки политики на управляемое устройство;
- список активных профилей политик с указанием их названий и приоритетов на момент доставки политики на управляемое устройство.

Вы можете использовать эту информацию, чтобы обеспечить применение правильной политики к устройству и в целях устранения неполадок. По умолчанию параметр выключен.

Защитить службу Агента администрирования от неавторизованного удаления, остановки или изменения параметров работы

Если этот параметр включен, после того, как Агент администрирования был установлен на управляемом устройстве, компонент не может быть удален или изменен без требуемых прав. Работа Агента администрирования не может быть остановлена. Этот параметр не влияет на контроллеры домена.

Включите этот параметр, чтобы защитить Агент администрирования на рабочих станциях, управляемых с правами локального администратора.

По умолчанию параметр выключен.

Использовать пароль деинсталляции

Если параметр включен, при нажатии на кнопку **Изменить** можно указать пароль для утилиты klmover и задачи удаленной деинсталляции Агента администрирования на устройствах с операционной системой Windows.

По умолчанию параметр выключен.

Хранилища

В разделе **Хранилища** можно выбрать типы объектов, информацию о которых Агент администрирования будет отправлять на Сервер администрирования:

Информация об установленных приложениях

Если этот параметр включен, на Сервер администрирования отправляется информация о приложениях, установленных на клиентских устройствах.

По умолчанию параметр включен.

Включить информацию о патчах

Информация о патчах приложений, установленных на клиентских устройствах, отправляется на Сервер администрирования. Включение этого параметра может увеличить нагрузку на Сервер администрирования и СУБД, а также вызвать увеличение объема базы данных.

По умолчанию параметр включен. Доступен только для Windows.

Информация об обновлениях Центра обновления Windows

Если параметр установлен, на Сервер администрирования отправляется информация об обязательных обновлениях Центра обновления Windows, которые необходимо установить на клиентских устройствах.

По умолчанию параметр включен. Доступен только для Windows.

Информация о необязательных обновлениях Microsoft Windows не отправляется на Сервер администрирования.

Информация об уязвимостях в приложениях и соответствующих обновлениях

Если этот параметр включен, информация об уязвимостях в приложениях сторонних производителей (включая программное обеспечение Microsoft), обнаруженных на управляемых устройствах, и об обновлениях программного обеспечения для закрытия уязвимостей (не включая программное обеспечение Microsoft) отправляется на Сервер администрирования.

Выбор этого параметра (**Информация об уязвимостях в приложениях и соответствующих обновлениях**) увеличивает нагрузку на сеть, загрузку диска Сервера администрирования и потребление ресурсов Агентом администрирования.

По умолчанию параметр включен. Доступен только для Windows.

Для управления обновлениями приложений Microsoft используйте параметр **Информация об обновлениях Центра обновления Windows**.

Информация о реестре оборудования

Установленный на устройстве Агент администрирования отправляет информацию об оборудовании устройства на Сервер администрирования. Вы можете просмотреть информацию об оборудовании в свойствах устройства.

Убедитесь, что утилита lshw установлена на устройствах Linux, с которых вы хотите получить информацию об оборудовании. Сведения об оборудовании, полученные с виртуальных машин, могут быть неполными в зависимости от используемого гипервизора

Если в политике Агента администрирования наложен запрет на изменение параметров, указанных в этом разделе, эти параметры недоступны для изменения.

Обновления и уязвимости в приложениях

В разделе **Обновления и уязвимости в приложениях** вы можете включить проверку исполняемых файлов на наличие уязвимостей:

Проверять исполняемые файлы на наличие уязвимостей при запуске

Если параметр включен, при запуске исполняемых файлов выполняется их проверка на наличие уязвимостей.

По умолчанию параметр включен.

Управление перезагрузкой

В разделе **Управление перезагрузкой** можно выбрать и настроить действие, если во время работы, установки или удаления приложения требуется перезагрузить операционную систему управляемого устройства:

Не перезагружать операционную систему

Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

При необходимости перезагрузить операционную систему автоматически

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

Запрашивать у пользователя

На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

Повторять запрос периодически через (мин)

Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

Принудительно перезагружать через (мин)

После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

Принудительно закрывать приложения в заблокированных сеансах

Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

Управление патчами и обновлениями

В разделе Управление патчами и обновлениями можно настроить получение и распространение обновлений и установку патчей на управляемые устройства:

Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"

Если флажок установлен, патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений.

Если флажок снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрен*.

По умолчанию параметр включен.

Скачивать обновления и антивирусные базы с Сервера администрирования заранее (рекомендуется)

Если параметр включен, офлайн-модель получения обновлений используется. Когда Сервер администрирования получает обновления, он уведомляет Агент администрирования (на устройствах, где он установлен) об обновлениях, которые потребуются для управляемых приложений. Когда Агенты администрирования получают информацию об обновлениях, они загружают нужные файлы с Сервера администрирования заранее. При первом соединении с Агентом администрирования Сервер инициирует загрузку обновлений этим Агентом. После того как Агент администрирования на клиентском устройстве загрузит все обновления, обновления становятся доступными для приложений на устройстве.

Когда управляемое приложение на клиентском устройстве обращается к Агенту администрирования за обновлениями, Агент проверяет, есть ли у него необходимые обновления. Если обновления были получены от Сервера администрирования не раньше, чем за 25 часов с момента запроса управляемого приложения, Агент администрирования не подключается к Серверу администрирования и предоставляет управляемому приложению обновления из локального кеша. Соединение с Сервером администрирования может не выполняться, когда Агент администрирования предоставляет обновления для приложений на клиентских устройствах, но подключение не требуется для обновления.

Если параметр выключен, офлайн-модель получения обновлений не используется. Обновления распространяются в соответствии с расписанием задачи загрузки обновлений.

По умолчанию параметр включен.

Подключения

Раздел **Подключения** включает три вложенных раздела:

- **Сеть**
- **Профили соединений**
- **Расписание соединений**

В разделе **Сеть** 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.

  Сжимать сетевой трафик

  Если параметр выключен, будет увеличена скорость передачи данных Агентом администрирования, сокращен объем передаваемой информации и уменьшена нагрузка на Сервер администрирования.

  > Нагрузка на центральный процессор клиентского компьютера может возрасти.

  По умолчанию флажок установлен.

  Открывать порты Агента администрирования в брандмауэре Microsoft Windows

Если параметр включен, порты, необходимые для работы Агента администрирования, будут добавлены в список исключений брандмауэра Microsoft Windows.

По умолчанию параметр включен.

Использовать SSL-соединение

Если этот параметр включен, подключение к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

По умолчанию параметр включен.

Использовать шлюз 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.

- **Использовать точку распространения для принудительного подключения к Серверу администрирования**

  Выберите этот параметр, если вы выбрали параметр **Использовать эту точку распространения в качестве push-сервера** в окне параметров точки распространения. Иначе точка распространения не будет выполнять роль push-сервера.

В подразделе **Профили соединений** 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

Вы можете просмотреть и добавить профили подключения Агента администрирования к Серверу администрирования. В этом разделе также можно сформировать правила переключения Агента администрирования на другие Серверы администрирования при возникновении следующих событий:

- подключении клиентского устройства к другой локальной сети;
- отключении устройства от локальной сети организации;
- изменении адреса шлюза соединения или изменении адреса DNS-сервера.

Включить автономный режим, когда Сервер администрирования недоступен

Если параметр включен, при подключении через этот профиль приложения, установленные на клиентском устройстве, будут использовать профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей. В случае, если для приложения политика для автономных пользователей не определена, приложение будет использовать активную политику.

Если параметр выключен, приложения будут использовать активные политики.

По умолчанию параметр выключен.

В разделе **Расписание соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования:

Подключаться при необходимости

Если выбран этот вариант, подключение будет устанавливаться тогда, когда Агенту администрирования нужно передать данные на Сервер администрирования.

По умолчанию выбран этот вариант.

Подключаться в указанные периоды

Если выбран этот вариант, подключение Агента администрирования к Серверу администрирования выполняется в заданные периоды времени. Можно добавить несколько периодов подключения.

Опрос сети точками распространения

В разделе **Опрос сети точками распространения** вы можете настроить автоматический опрос сети. Вы можете использовать следующие параметры, чтобы включить опрос и настроить его расписание:

Сеть Windows

Параметр доступен только для точек распространения с операционной системой Windows.

Если этот параметр включен, Сервер администрирования автоматически опрашивает сеть в соответствии с расписанием, настроенным по ссылкам **Настроить расписание быстрого опроса** и **Настроить расписание полного опроса**.

Если этот параметр выключен, Сервер администрирования опрашивает сеть с указанным периодом в поле **Период опроса сети (мин)**.

Период обнаружения устройств для Агента администрирования можно настроить в полях **Период опроса Windows-доменов (мин)** (для быстрого опроса сети Windows) и **Период опроса сети (мин)** (для полного опроса сети Windows).

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.

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.

Контроллеры доменов

Если этот параметр включен, точка распространения автоматически выполняет опрос контроллеров домена в соответствии с расписанием, настроенным по кнопке **Настроить расписание опроса**.

Если параметр выключен, точка распространения не выполняет опрос контроллеров домена.

Периодичность опроса контроллеров домена для версий Агента администрирования ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если этот параметр включен.

По умолчанию параметр выключен.

Параметры сети для точек распространения

В разделе **Параметры сети для точек распространения** вы можете указать параметры доступа к интернету:

- **Использовать прокси-сервер**

  Если этот параметр включен, для подключения точек распространения к серверу обновлений "Лаборатории Касперского" используется прокси-сервер в интернете.

- **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.

Прокси-сервер KSN (точки распространения)

В разделе **Прокси-сервер KSN (точки распространения)** вы можете настроить приложение так, чтобы точка распространения использовалась для пересылки Kaspersky Security Network (KSN) запросов от управляемых устройств:

Включить прокси-сервер KSN на стороне точки распространения

Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского".

По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены в окне свойств Сервера администрирования.

Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

Пересылать KSN запрос Серверу администрирования

Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

По умолчанию параметр включен.

Доступ к облачной службе KSN/KPSN непосредственно через интернет

Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или KPSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или KPSN.

TCP-порт

Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.

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.

HTTPS-порт

Если вам нужно, чтобы управляемые устройства подключались к прокси-серверу KSN через порт HTTPS, включите параметр **Использовать HTTPS** и укажите номер порта в поле **HTTPS-порт**. По умолчанию параметр выключен. По умолчанию подключение к прокси-серверу KSN выполняется через HTTPS-порт 17111.

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".

Управление учетными записями (только для Linux)

Раздел **Управление учетными записями (только для Linux)** состоит из трех подразделов:

- **Управление пользовательскими сертификатами**
- **Добавление или изменение групп локальных администраторов**
- **Загрузка референсного файла, для защиты файла sudoers на устройстве пользователя от изменений**

В подразделе **Управление пользовательскими сертификатами** вы можете указать, какие корневые сертификаты устанавливать. Эти сертификаты могут использоваться, например, для проверки подлинности веб-сайтов или веб-серверов.

Установить корневые сертификаты

Если этот параметр включен, сертификаты, добавленные в таблицу, будут установлены на указанных устройствах.

Если этот параметр выключен, сертификаты не будут установлены на указанные устройства.

По умолчанию параметр выключен.

Добавить

Нажав на эту кнопку открывается окно, в котором можно добавить сертификат.

Размер сертификата должен быть меньше 10 МБ.

Kaspersky Security Center поддерживает сертификаты с расширениями CER, CRT, CERT, PEM и KEY.

В подразделе **Добавление или изменение групп локальных администраторов** вы можете управлять группами локальных администраторов. Эти группы используются, например, при отзыве прав локального администратора. Вы также можете проверить список учетных записей привилегированных пользователей, используя **Отчет о привилегированных пользователях устройств (только для Linux)**.

Добавить

Нажмите на эту кнопку, чтобы добавить локальную группу администраторов.

Изменить

Нажмите на эту кнопку, чтобы изменить локальную группу администраторов.

Эта кнопка доступна, если установлен флажок рядом с группой локальных администраторов.

Удалить

Нажмите на эту кнопку, чтобы удалить выбранную группу локальных администраторов из таблицы.

Эта кнопка доступна, если установлен флажок рядом с группой локальных администраторов.

В подразделе **Загрузка референсного файла, для защиты файла sudoers на устройстве пользователя от изменений** вы можете настроить управление файлом sudoers. Привилегированные группы и пользователи устройства определяются файлом sudoers на устройстве. Файл sudoers находится в папке `/etc/sudoers`. Вы можете загрузить референсный файл sudoers, чтобы защитить файл sudoers от изменений. Это предотвратит нежелательные изменения файла sudoers.

Недопустимый референсный файл sudoers может привести к неисправности устройства пользователя.

Контролировать файл sudoers

Если этот параметр включен, файл sudoers будет заменен текущим референсным файлом sudoers.

Если этот параметр выключен, файл sudoers остается без изменений.

По умолчанию параметр выключен.

Референсный файл sudoers

В этом поле отображается название загруженного референсного файла sudoers.

Загрузить

Нажмите на эту кнопку, чтобы загрузить референсный файл sudoers.

Текущий референсный файл sudoers

Нажмите на эту кнопку, чтобы просмотреть текущий файл sudoers.

История ревизий

На вкладке **История ревизий** вы можете:

- Просмотреть и сохранить историю изменений политики.
- Откатить к ревизии политики.
- Добавить и изменить описание ревизии политики.
- Сравнить ревизии политики.

Использование Агента администрирования для Windows, Linux и macOS: сравнение

Использование Агента администрирования зависит от операционной системы устройства. Свойства политики Агента администрирования и инсталляционного пакета зависят от операционной системы. В таблице ниже сравниваются возможности и сценарии использования Агента администрирования, доступные для операционных систем Windows, Linux и macOS.

Функция Агента администрирования	Windows	Linux	macOS
Установка			
Установка методом клонирования образа жесткого диска администратора с операционной системой и Агентом администрирования сторонними средствами	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓	✓
Установка приложений с помощью сторонних средств удаленной установки приложений	✓	✓	✓
Установка вручную с помощью запуска инсталляторов приложений на устройствах	✓	✓	✓
Установка Агента администрирования в тихом режиме	✓	✓	✓
Подключение клиентского устройства к Серверу администрирования вручную	✓	✓	✓
Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center	✓	✓ Ограничение: не поддерживается Агентом администрирования Elbrus Edition.	—
Автоматическое распространение ключа	✓	✓	✓
Принудительная синхронизация	✓	✓	✓ За исключением push-сервера
Точка распространения			
Использование точки распространения	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓ Ограничение: не поддерживается Агентом администрирования Elbrus Edition.	✓
Расчет количества и конфигурации точек распространения	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓ Без использования Network Location Awareness (NLA). Ограничение: не поддерживается Агентом администрирования Elbrus Edition.	✓ Без использования Network Location Awareness (NLA).
Офлайн-модель получения обновлений	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓ Ограничение: не поддерживается Агентом администрирования Elbrus Edition.	✓
Опрос сети	✓ • Опрос IP-диапазонов • Опрос контроллеров домена (Microsoft Active Directory) Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓ Опрос IP-диапазонов Опрос Zeroconf Опрос контроллеров домена (Microsoft Active Directory, Samba 4 Active Directory, FreeIPA, ALD Pro) Ограничение: не поддерживается Агентом администрирования Elbrus Edition.	—

Функция Агента администрирования	Windows	Linux	macOS
Запуск службы прокси-сервер KSN на стороне точки распространения	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓ Ограничение: не поддерживается Агентом администрирования Elbrus Edition.	—
Загрузка обновлений через серверы обновлений "Лаборатории Касперского" в хранилища точек распространения, которые распространяют обновления на управляемые устройства	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓ Ограничение: не поддерживается Агентом администрирования Elbrus Edition.	— Если устройства с операционной системой Linux или macOS находятся в области действия задачи Загрузка обновлений в хранилища точек распространения, задача завершится со статусом Сбой, даже если она успешно завершилась на всех устройствах с операционной системой Windows.
Принудительная установка приложений	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	С ограничением: невозможно выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой Linux. Не поддерживается Агентом администрирования Elbrus Edition.	С ограничением: невозможно выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой macOS.
Использовать в качестве push-сервера	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓ Ограничение: не поддерживается Агентом администрирования Elbrus Edition.	—
Работа с приложениями сторонних производителей			
Удаленная установка приложений на устройства	✓	✓ Ограничение: не поддерживается Агентом администрирования Elbrus Edition.	✓ Подробнее см. в статье Удаленная установка приложений на устройства с операционной системой macOS.
Настройка обновлений операционной системы в политике Агента администрирования	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	—	—
Просмотр информации об уязвимостях в приложениях	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	—	—
Поиск уязвимостей в приложениях	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	—	—
Обновления программного обеспечения	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	—	—
Инвентаризация программного обеспечения, установленного на устройствах	✓	✓	—
Виртуальные машины			

Функция Агента администрирования	Windows	Linux	macOS
Установка Агента администрирования на виртуальные машины	✓	✓ Ограничение: не поддерживается Агентом администрирования Elbrus Edition.	✓
Оптимизация параметров для VDI	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓ Ограничение: не поддерживается Агентом администрирования Elbrus Edition.	✓
Поддержка динамических виртуальных машин	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓ Ограничение: не поддерживается Агентом администрирования Elbrus Edition.	✓
Другое			
Аудит действий на удаленном клиентском устройстве с помощью совместного доступа к рабочему столу Windows	✓	—	—
Мониторинг состояния антивирусной защиты	✓	✓ Ограничение: не поддерживается Агентом администрирования Elbrus Edition.	✓
Управление перезагрузкой устройств	✓	—	—
Поддержка отката файловой системы	✓	✓	✓
Использование Агента администрирования в качестве шлюза соединений	✓	✓	✓
Менеджер соединений	✓	✓	✓
Профили соединения для автономных пользователей	✓	✓	✓
Переключение Агента администрирования с одного Сервера администрирования на другой (автоматически по сетевому местоположению)	✓	✓	✓
Проверка соединения клиентского устройства с Сервером администрирования. Утилита klnagchk	✓	✓	✓
Удаленное подключение к рабочему столу клиентского устройства	✓	✓ Ограничение: не поддерживается Агентом администрирования Elbrus Edition.	✓ С помощью системы Virtual Network Computing (VNC).

Функция Агента администрирования	Windows	Linux	macOS
Загрузка автономного инсталляционного пакета с помощью мастера переноса данных	✓	✓	✓
Просмотр информации об аппаратном обеспечении клиентских устройств	✓	✓ Информация об аппаратном обеспечении устройств с операционной системой Linux передается на Сервер администрирования Агентом администрирования, который установлен на этих устройствах, и ограничивается информацией, указанной в описании параметров управляемого устройства.	✓ Информация об аппаратном обеспечении устройств с операционной системой macOS передается на Сервер администрирования Агентом администрирования, который установлен на этих устройствах, и ограничивается информацией, указанной в описании параметров управляемого устройства.

Сравнение параметров Агента администрирования по операционным системам

В таблице ниже описано, какие параметры политики Агента администрирования доступны в зависимости от операционной системы управляемого устройства, на котором установлен Агент администрирования.

Параметры Агента администрирования: сравнение по операционным системам

Раздел Параметры	Windows	Linux	macOS
Общие	✓	✓	✓
Настройка событий	✓	✓	✓
Параметры	✓	✓ Доступны следующие параметры: • **Распространять файлы только через точки распространения** • **Максимальный размер очереди событий (МБ)** • **Приложение может получать расширенные данные политики на устройстве**	✓
Хранилища	✓	✓ Доступна функциональность: • **Информация об установленных приложениях** • **Информация о реестре оборудования**	✓ Функциональность **Информация о реестре оборудования** доступна.
Подключения → Сеть	✓	✓ Кроме параметра **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**.	✓
Подключения → Профили соединений	✓	✓	✓
Подключения → Расписание соединений	✓	✓	✓

Раздел Параметры	Windows	Linux	macOS
Опрос сети точками распространения	✓ Доступны следующие параметры: • **Сеть Windows** • **IP-диапазоны** • **Контроллеры доменов**	✓ Доступны следующие параметры: • **Zeroconf** • **IP-диапазоны** • **Контроллеры доменов**	—
Параметры сети для точек распространения	✓	✓	✓
Прокси-сервер KSN (точки распространения)	✓	✓	—
Обновления (точки распространения)	✓	✓	—
История ревизий	✓	✓	✓

Включение и выключение режима низкого потребления ресурсов для Агента администрирования

Режим низкого потребления ресурсов позволяет ограничить использование оперативной памяти Агента администрирования, установленного на клиентском устройстве. По умолчанию режим низкого потребления ресурсов выключен.

В режиме низкого потребления ресурсов не выполняются следующие функции:

- Агент администрирования не может быть назначен точкой распространения (вручную или автоматически).
- Агент администрирования не записывает информацию о состоянии Агента администрирования в отдельный текстовый файл.
- Агент администрирования не поддерживает офлайн-модель получения обновлений.
- Следующие компоненты и процессы выключены:
  - Получение информации о сторонних обновлениях и уязвимостях.
  - Запуск прокси-сервера KSN на стороне точки распространения.
  - Загрузка обновлений в хранилище точки распространения.
  - Не использование блокировки DNS-сервера.
  - Получение информации о свободном месте на диске.

Компоненты и процессы возобновляют работу после выключения режима низкого потребления ресурсов.

Чтобы включить режим низкого потребления ресурсов:

1. Выполните следующую команду в командной строке на клиентском устройстве:

   ```
   sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. Перезапустите Агент администрирования с помощью следующей команды:

   ```
   sudo service klnagent64 restart
   ```

3. В журнале событий операционной системы проверьте, отображается ли запись о том, что **Агент администрирования Kaspersky Security Center работает в режиме низкого потребления ресурсов**.

Режим низкого потребления ресурсов включен.

Чтобы выключить режим низкого потребления ресурсов:

1. Выполните следующую команду в командной строке на клиентском устройстве:

   ```
   sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. Перезапустите Агент администрирования с помощью следующей команды:

   ```
   sudo service klnagent64 restart
   ```

Режим низкого потребления ресурсов выключен.

Также можно включить режим низкого потребления ресурсов удаленно с помощью задачи *Удаленное выполнение скриптов*.

Настройка параметров защиты управляемых приложений

Для настройки параметров защиты управляемых приложений "Лаборатории Касперского" вы можете использовать политики.

Подробнее о настройке политик Kaspersky Endpoint Security см. в соответствующей справке:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux
- Справка Kaspersky Endpoint Security для Mac

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**.

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.

Kaspersky Security Network (KSN)

В этом разделе описано использование инфраструктуры онлайн-служб Kaspersky Security Network (KSN). Приведена информация о KSN, а также инструкции по включению KSN, настройке доступа к KSN, по просмотру статистики использования прокси-сервера KSN.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

О KSN

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. KSN позволяет получать из репутационных баз "Лаборатории Касперского" информацию о приложениях, установленных на управляемых устройствах.

Участвуя в Kaspersky Security Network, вы соглашаетесь автоматически предоставлять "Лаборатории Касперского" информацию о работе приложений безопасности, установленных на компьютерах и мобильных устройствах, управление которыми осуществляется с помощью Kaspersky Security Center Linux. Передача информации выполняется в соответствии с настроенными параметрами доступа к KSN.

Kaspersky Security Center Linux поддерживает следующие инфраструктурные решения KSN:

- *Глобальный KSN* – решение, позволяющее обмениваться информацией с Kaspersky Security Network. Участвуя в программе KSN, вы соглашаетесь в автоматическом режиме предоставлять в "Лабораторию Касперского" информацию о работе приложений "Лаборатории Касперского", установленных на клиентских устройствах, находящихся под управлением Kaspersky Security Center Linux. Передача информации выполняется в соответствии с настроенными параметрами доступа к KSN. Специалисты "Лаборатории Касперского" дополнительно анализируют полученную информацию и включают ее в репутационные и статистические базы данных Kaspersky Security Network. Kaspersky Security Center Linux использует это решение по умолчанию.

- *Kaspersky Private Security Network (KPSN)* – это решение, которое предоставляет пользователям устройств с установленными приложениями "Лаборатории Касперского" доступ к репутационным базам Kaspersky Security Network и другим статистическим данным без отправки данных со своих устройств в Глобальный KSN. KPSN предназначен для организаций, которые не могут участвовать в Kaspersky Security Network по одной из следующих причин:

  - Устройства пользователей не подключены к интернету.

  - Передача любых данных за пределы страны или корпоративной сети (LAN) запрещена законом или корпоративными политиками безопасности.

  Вы можете настроить параметры доступа Kaspersky Private Security Network в разделе **Прокси-сервер KSN** окна свойств Сервера администрирования.

Приложение предлагает присоединиться к KSN во время работы мастера первоначальной настройки. Вы можете начать использование KSN или отказаться от использования KSN в любой момент работы с приложением.

Вы используете KSN в соответствии с Положением о KSN, которое вы читаете и принимаете при включении KSN. Если Положение о KSN обновлено, оно отображается при обновлении Сервера администрирования с предыдущей версии. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с предыдущей версией Положения о KSN, которую вы приняли ранее.

Когда KSN включен, Kaspersky Security Center Linux проверяет доступность серверов KSN, чтобы убедиться, что уровень безопасности для управляемых устройств поддерживается. Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы.

Клиентские устройства, находящиеся под управлением Сервера администрирования, взаимодействуют с KSN при помощи службы прокси-сервера KSN. Служба прокси-сервера KSN предоставляет следующие возможности:

- Клиентские устройства могут выполнять запросы к KSN, получать информацию от KSN и передавать в KSN информацию, даже если они не имеют прямого доступа в интернет.

- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентским устройством запрошенной информации.

Вы можете настроить параметры прокси-сервера KSN в разделе **Прокси-сервер KSN** окна свойств Сервера администрирования.

Настройка доступа к KSN

Можно задать доступ к Kaspersky Security Network (KSN) из свойств Сервера администрирования, из политики Сервера администрирования и с точки распространения.

Чтобы настроить доступ Сервера администрирования к KSN из свойств Сервера Администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Прокси-сервер KSN**.

3. Переведите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования Включено**

   Если этот параметр включен, прокси-сервер KSN отправляет данные в KSN для повышения эффективности работы компонентов Kaspersky Security Center и приложений "Лаборатории Касперского". Передача данных от клиентских устройств в KSN регулируется политикой Kaspersky Endpoint Security, действующей на клиентских устройствах. Если переключатель выключен, передача данных в KSN от Сервера администрирования и от клиентских устройств через Kaspersky Security Center Linux не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky Security Center Linux). Действующая на клиентских устройствах политика Kaspersky Endpoint Security определяет, какие данные эти устройства напрямую (не через Kaspersky Security Center Linux) передают в KSN.

4. Выберите решение инфраструктуры KSN.

   В подразделе **Участие в KSN** выполните одно из следующих действий:

   - Если вы используете Глобальный KSN, переведите переключатель в положение **Использовать Kaspersky Security Network Включено**.

     При включении этого параметра убедитесь, что вы прочитали и принимаете условия Положения о KSN.

   - Если вы используете KPSN, переведите переключатель в положение **Использовать Kaspersky Private Security Network Включено** и нажмите на кнопку **Файл с параметрами прокси-сервера KSN**, чтобы загрузить параметры KPSN (файлы с расширениями pkcs7 и pem). После загрузки параметров в интерфейсе отображаются наименование провайдера, контакты провайдера и дата создания файла с параметрами KPSN.

   При переводе переключателя в положение **Использовать Kaspersky Private Security Network Включено** появится сообщение с подробной информацией о KPSN.

   KPSN поддерживают следующие приложения "Лаборатории Касперского":

   - Kaspersky Security Center Linux
   - Kaspersky Endpoint Security для Linux
   - Kaspersky Endpoint Security для Windows

   Если вы включите KPSN в Kaspersky Security Center Linux, эти приложения получат об этом информацию о поддержке KPSN. В окне свойств приложения в подразделе **Kaspersky Security Network** раздела **Продвинутая защита** отображается поставщик KSN: KSN или KPSN.

Kaspersky Security Center Linux не отправляет статистику Kaspersky Security Network, если настроен KPSN в окне свойств Сервера администрирования в разделе **Прокси-сервер KSN**.

5. Установите флажок **Игнорировать параметры прокси-сервера для подключения к KPSN**, если параметры прокси-сервера настроены в свойствах Сервера администрирования, но ваша архитектура сети требует, чтобы вы использовали KPSN напрямую. В противном случае запрос от управляемого приложения не будет передан в KPSN.

6. Настройте параметры подключения Сервера администрирования к службе прокси-сервера KSN:

   - В блоке **Подключение**, в поле ввода **TCP-порт**, укажите номер TCP-порта, через который будет выполняться подключение к прокси-серверу KSN. По умолчанию подключение к прокси-серверу KSN выполняется через порт 13111.

   - Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, выберите параметр **Использовать UDP-порт** и в поле **UDP-порт** укажите номер порта. По умолчанию параметр выключен, используется порт TCP. Если параметр включен, по умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

   - Чтобы Сервер администрирования подключался к прокси-серверу KSN через HTTPS-порт, выберите параметр **Использовать HTTPS** и в поле **HTTPS-порт** укажите номер порта. По умолчанию параметр выключен, используется порт TCP. Если параметр включен, по умолчанию подключение к прокси-серверу KSN выполняется через HTTPS-порт 17111.

     Если вы выбираете этот параметр, включите использование протокола HTTPS на всех точках распространения, выполняющих роль прокси-сервера KSN. Это позволяет избежать превышения нагрузки на прокси-сервер.

7. Включите переключатель **Подключать подчиненные Серверы администрирования к KSN через главный Сервер**.

   Если этот параметр включен, подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера KSN. Если этот параметр выключен, подчиненные Серверы администрирования подключаются к KSN самостоятельно. В этом случае управляемые устройства используют подчиненные Серверы администрирования как прокси-серверы KSN.

   Подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера, если в свойствах подчиненных Серверов администрирования в разделе **Прокси-сервер KSN** также переключатель переведен в положение **Включить прокси-сервер KSN на Сервере администрирования Включено**.

8. Нажмите на кнопку **Сохранить**.

Параметры доступа к KSN будут сохранены.

Чтобы настроить доступ Сервера администрирования к KSN из политики Сервера Администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами → Политики**.

2. Выберите политику Сервера Администрирования.

3. В открывшемся окне свойств политики перейдите на вкладку **Параметры приложения**.

4. Выберите раздел **Прокси-сервер KSN** и выполните действия, описанные в пунктах 3-8 в инструкции выше.

Параметры доступа к KSN будут сохранены.

Можно также настроить доступ к KSN со стороны точки распространения, например, если необходимо снизить нагрузку на Сервер администрирования. Точка распространения, выполняющая роль прокси-сервера KSN, отправляет KSN запросы от управляемых устройств напрямую в "Лабораторию Касперского", минуя Сервер администрирования.

Чтобы настроить доступ точки распространения к Kaspersky Security Network (KSN):

1. Убедитесь, что точка распространения была назначена вручную.

2. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

3. На вкладке **Общие** выберите раздел **Точки распространения**.

4. Нажмите на имя точки распространения, чтобы открыть окно ее свойств.

5. В окне свойств точки распространения в разделе **Прокси-сервер KSN**, включите параметр **Включить прокси-сервер KSN на стороне точки распространения** и параметр **Доступ к облачной службе KSN/KPSN непосредственно через интернет**.

6. Нажмите на кнопку **ОК**.

Точка распространения будет исполнять роль прокси-сервера KSN.

Обратите внимание, что точка распространения не поддерживает проверку подлинности управляемого устройства по протоколу NTLM.

Включение и выключение использования KSN

Чтобы включить использование KSN:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Прокси-сервер KSN**.

3. Переведите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования Включено**.

Прокси-сервер KSN включен и отправляет данные в KSN для повышения эффективности работы компонентов Kaspersky Security Center и производительности приложений "Лаборатории Касперского".

1. В зависимости от используемого решения инфраструктуры KSN, включите соответствующие переключатели.

   - Если вы используете Глобальный KSN, переведите переключатель в положение **Использовать Kaspersky Security Network Включено**.

     Теперь доступна отправка данных в KSN. При включении этого параметра, вам нужно прочитать и принять условия Положения о KSN.

   - Если вы используете KPSN, переведите переключатель в положение **Использовать Kaspersky Private Security Network Включено** и нажмите на кнопку **Файл с параметрами прокси-сервера KSN**, чтобы загрузить параметры KPSN (файлы с расширениями pkcs7 и pem). После загрузки параметров в интерфейсе отображаются наименование провайдера, контакты провайдера и дата создания файла с параметрами KPSN.

     При переводе переключателя в положение **Использовать Kaspersky Private Security Network Включено** появится сообщение с подробной информацией о KPSN.

2. Нажмите на кнопку **Сохранить**.

Чтобы выключить использование KSN:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Прокси-сервер KSN**.

3. Переведите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования Выключено**, чтобы выключить службу прокси-сервера KSN.

4. Нажмите на кнопку **Сохранить**.

Просмотр принятого Положения о KSN

При включении Kaspersky Security Network (KSN) вам нужно прочитать и принять Положение о KSN. Вы можете просмотреть принятое Положение о KSN в любое время.

Чтобы просмотреть принятое Положение о KSN:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Прокси-сервер KSN**.

3. Перейдите по ссылке **Просмотреть Положение о Kaspersky Security Network**.

В открывшемся окне вы можете просмотреть текст принятого Положения о KSN.

Принятие обновленного Положения о KSN

Вы используете KSN в соответствии с Положением о KSN, которое вы читаете и принимаете при включении KSN. Если Положение о KSN обновлено, оно отображается при обновлении Сервера администрирования с предыдущей версии. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с версией Положения о KSN, которую вы приняли ранее.

После обновления Сервера администрирования с предыдущей версии обновленное Положение о KSN отображается автоматически. Если вы отклоните обновленное Положение о KSN, вы все равно сможете просмотреть и принять его позже.

Чтобы просмотреть и принять или отклонить обновленное Положение о KSN:

1. Нажмите на значок **Просмотреть уведомления о событиях** в правом верхнем углу главного окна приложения.

   Откроется окно **Уведомления**.

2. Перейдите по ссылке **Просмотреть обновленное Положение о KSN**.

   Откроется окно **Обновление Положения о Kaspersky Security Network**.

3. Прочтите Положение о KSN, а затем примите решение, нажав одну из следующих кнопок:

   - **Я принимаю условия обновленного Положения о KSN**
   - **Использовать KSN со старым Положением о KSN**

   В зависимости от вашего выбора KSN продолжит работу в соответствии с условиями текущего или обновленного Положения о KSN. Вы можете в любой момент просмотреть текст принятого Положения о KSN в свойствах Сервера администрирования.

Проверка, работает ли точка распространения как прокси-сервер KSN

На управляемом устройстве, которое выполняет роль точки распространения, вы можете включить прокси-сервер Kaspersky Security Network (KSN). Управляемое устройство работает как прокси-сервер KSN, если на нем запущена служба ksnproxy. Вы можете, проверить включить или выключить эту службу на устройстве локально.

Вы можете назначить устройство с операционной системой Windows или Linux в качестве точки распространения. Способ проверки точки распространения зависит от операционной системы этой точки распространения.

Чтобы проверить, работает ли точка распространения с операционной системой Linux как прокси-сервер KSN:

1. На устройстве точки распространения выполните команду `ps aux`, чтобы отобразить список запущенных процессов.

2. В списке запущенных процессов проверьте, запущен ли процесс `/opt/kaspersky/klnagent64/sbin/ksnproxy`.

Если процесс `/opt/kaspersky/klnagent64/sbin/ksnproxy` запущен, Агент администрирования на устройстве участвует в Kaspersky Security Network и работает как прокси-сервер KSN для управляемых устройств, входящих в область применения точки распространения.

Чтобы проверить, работает ли точка распространения с операционной системой Windows как прокси-сервер KSN:

1. На устройстве, которое выполняет роль точки распространения, в Windows откройте окно **Службы** (**Все приложения** → **Администрирование** → **Службы**).

2. В списке служб проверьте, запущена ли служба прокси-сервера KSN – ksnproxy.

   Если служба ksnproxy запущена, то Агент администрирования на устройстве участвует в Kaspersky Security Network и работает как прокси-сервер KSN Proxy для управляемых устройств, входящих в область действия точки распространения.

При необходимости службу ksnproxy можно выключить. В этом случае Агент администрирования на точке распространения больше не участвует в Kaspersky Security Network. Для этого требуются права локального администратора.

Просмотр статистики работы прокси-сервера KSN

Kaspersky Security Center Web Console позволяет просматривать статистику использования прокси-сервера KSN.

Статистика включает следующие параметры:

- статус соединения с KSN;
- количество записей в кеше;
- количество пакетов, обработанных в кеше;
- количество полученных пакетов.

Если вы используете KPSN в качестве инфраструктурного решения, отображается статистика использования KPSN.

Чтобы просмотреть статистику:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Прокси-сервер KSN** и откройте вкладку **Статистика**.

   На вкладке отображается актуальная статистика использования прокси-сервера KSN. Статистика обновляется каждые 15 секунд.

Вы можете скопировать статистику, нажав на кнопку **Копировать в буфер обмена**.

Управление задачами

В этом разделе описаны задачи, которые используются в Kaspersky Security Center Linux.

О задачах

Kaspersky Security Center Linux управляет работой приложений безопасности "Лаборатории Касперского", установленных на устройствах, путем создания и запуска *задач*. С помощью задач выполняются установка, запуск и остановка приложений, проверка файлов, обновление баз и модулей приложений, другие действия с приложениями.

Вы можете создать задачу для приложения в Kaspersky Security Center Web Console, только если для этого приложения установлен плагин управления на сервере Kaspersky Security Center Web Console.

Задачи могут выполняться на Сервере администрирования и на устройствах.

Задачи, которые выполняются на Сервере администрирования, включают:

- автоматическая рассылка отчетов;
- загрузку обновлений в хранилище;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных.

На устройствах выполняются следующие типы задач:

- *Локальные задачи* – это задачи, которые выполняются на конкретном устройстве.

  Локальные задачи могут быть изменены не только администратором с помощью Kaspersky Security Center Web Console, но и пользователем удаленного устройства (например, в интерфейсе приложения безопасности). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором, как более приоритетные.

- *Групповые задачи* – это задачи, которые выполняются на всех устройствах указанной группы.

  Если иное не указано в свойствах задачи, групповая задача также распространяется на подгруппы указанной группы. Групповые задачи также действуют (опционально) и на устройства, подключенные к подчиненным и виртуальным Серверам администрирования, размещенным в этой группе и подгруппах.

- *Глобальные задачи* – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.

Для каждого приложения вы можете создавать любое количество групповых задач, глобальных задач и локальных задач.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

Запуск задач на устройстве выполняется только в том случае, если запущено приложение, для которого созданы эти задачи.

Результаты выполнения задач сохраняются в журнале событий операционной системы на каждом устройстве, в журнале событий на Сервере администрирования и в базе данных Сервера администрирования.

Не используйте в параметрах задач конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

Область задачи

Область применения 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. Также можно выбрать устройства, обнаруженные в сети Сервером администрирования.

- 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.

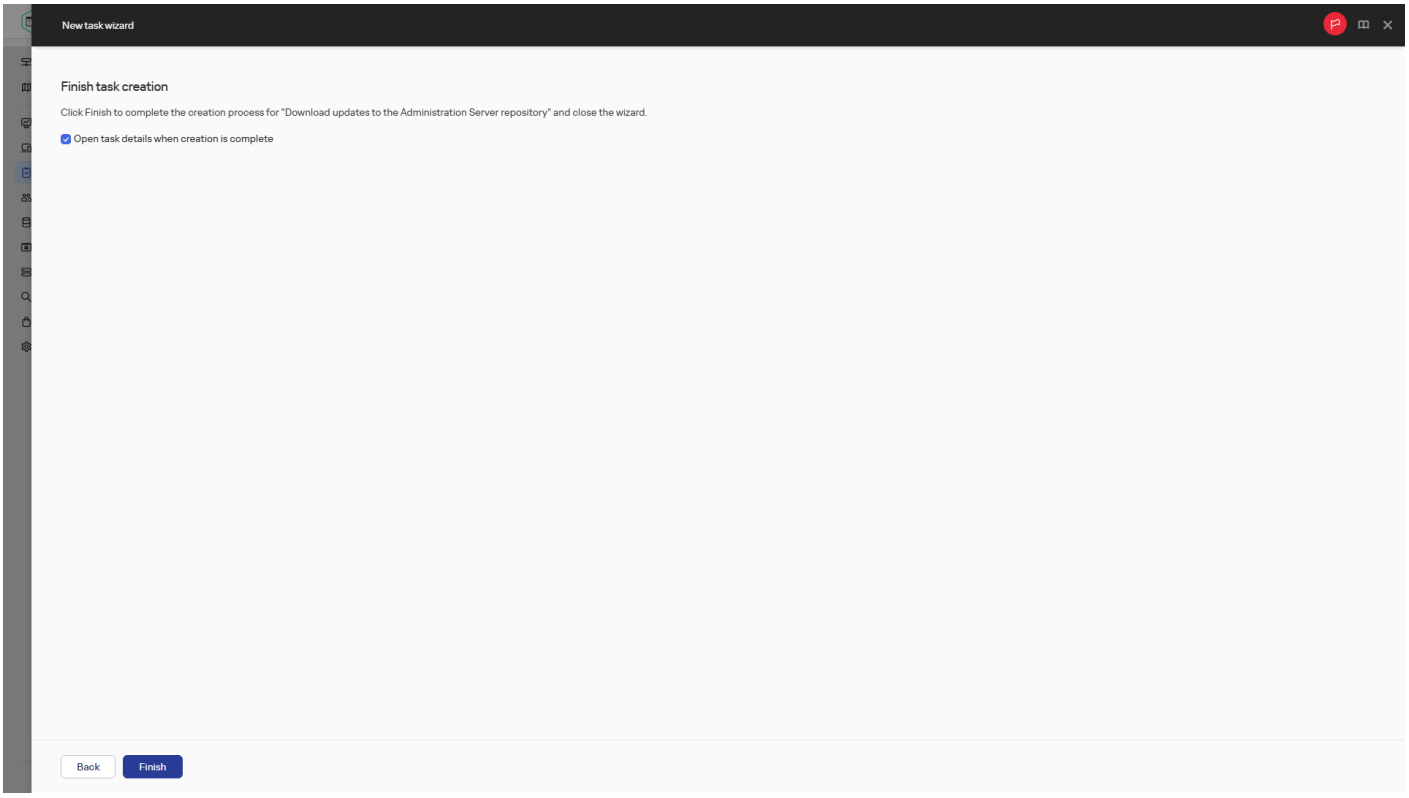
Создание задачи

Чтобы создать задачу:

1. В главном окне приложения перейдите в раздел **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.



Завершение создания задачи

Чтобы создать задачу, назначенную выбранным устройствам:

1. В главном окне приложения перейдите в раздел **Управление активами** → **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

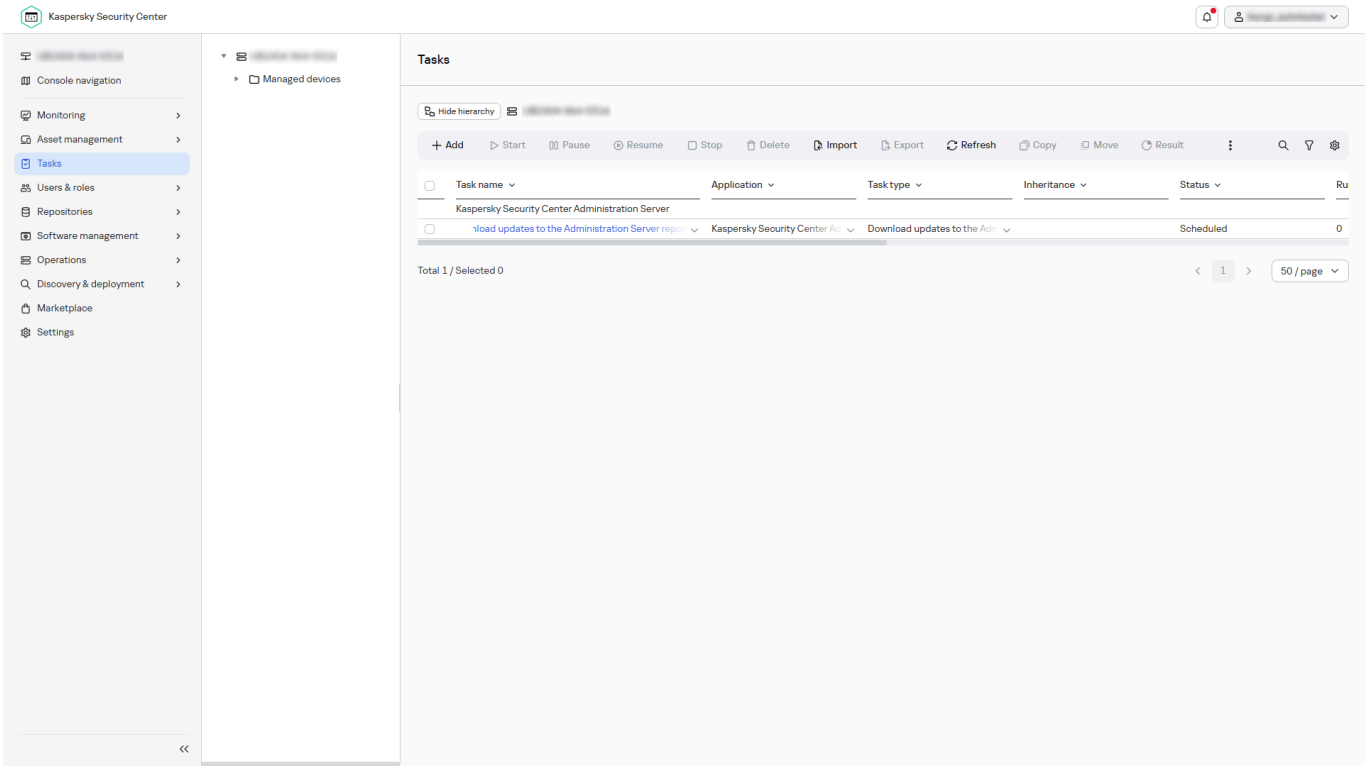
Приложение запускает задачи в соответствии с расписанием, заданным в свойствах каждой задачи. Вы можете запустить задачу вручную в любое время из списка задач. Также можно выбрать устройства в списке **Управляемые устройства** и запустить для них существующую задачу.

Чтобы запустить задачу вручную:

1. В главном окне приложения перейдите в раздел **Задачи**.

2. В отобразившемся списке задач установите флажок напротив задачи, которую вы хотите запустить.

3. Нажмите на кнопку **Запустить**.



Запуск задачи из списка задач

Задача будет запущена. Вы можете проверить статус задачи в столбце **Статус** или нажав на кнопку **Результат выполнения**.

Запуск задачи для выбранных устройств

Вы можете выбрать одно или несколько клиентских устройств в списке устройств, а затем запустить для них ранее созданную задачу. Это позволяет запускать задачи, созданные ранее для заданного набора устройств.

Это действие изменит в задаче список устройств, к которым применяется эта задача.
Старая область действия задачи будет удалена и заменена на выбранную.

Чтобы запустить задачу для выбранных устройств:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.
   Отобразится список управляемых устройств.

2. В списке управляемых устройств с помощью флажков выберите устройства, для которых будет выполняться задача. Вы можете использовать функции поиска и фильтрации, чтобы найти необходимые устройства.

3. Нажмите на кнопку **Запустить задачу** и выберите **Использовать существующую задачу**.

   Отобразится список существующих задач.

4. Выбранные устройства отображаются над списком задач. При необходимости вы можете удалить устройство из этого списка. Вы можете удалить все устройства, кроме одного.

5. Выберите необходимую задачу в списке. Вы можете использовать поле поиска над списком для поиска задачи по ее названию. Можно выбрать только одну задачу.

6. Сохраните изменения, нажав на одну из кнопок:

   - **Запустить и закрыть**

     Задача запускается для выбранных устройств.

   - **Запустить и открыть задачу**

     Задача запускается для выбранных устройств и отображается окно свойств задачи, где вы можете быстро просмотреть результаты ее выполнения.

Параметры запуска по расписанию в задаче не меняются.

Просмотр списка задач

Вы можете просмотреть список задач, созданных в Kaspersky Security Center Linux.

Чтобы просмотреть список задач,

В главном окне приложения перейдите в раздел **Задачи**.

Отобразится список задач. Задачи сгруппированы по названиям приложений, к которыми они относятся. Например, задача *Удаленная установка приложения* относится к Серверу администрирования, а задача *Обновление* относится к Kaspersky Endpoint Security.

Чтобы просмотреть свойства задачи,

нажмите на название задачи.

Окно свойств задачи отображается с несколькими именными вкладками. Например, **Тип задачи** отображается на вкладке **Общие**, а расписание задачи на вкладке **Расписание**.

Общие параметры задач

Этот раздел содержит описание параметров, которые вы можете просмотреть и настроить для большинства ваших задач. Список доступных параметров зависит от настраиваемой задачи.

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- Параметры перезагрузки операционной системы:

  Не перезагружать устройство

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

  Перезагрузить устройство

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

  Принудительно закрывать приложения в заблокированных сеансах

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.

- Параметры расписания задачи:

  Типы расписаний могут изменяться в зависимости от задачи.

Некоторые типы расписаний могут быть недоступны для других приложений "Лаборатории Касперского".

- **Параметры Запуск задачи:**

  Каждый N час

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые 6 часов, начиная с текущих системной даты и времени.

  Каждые N дней

  Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются приложением, для которого вы создаете задачу.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

  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.

  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.

  Один раз

  Задача выполняется один раз, в указанные дату и время (по умолчанию в день создания задачи).

  Немедленно

  Задача запускается сразу после сохранения ее параметров.

  Ежемесячно в выбранный день

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

По умолчанию указано время 18:00 и не выбраны дни месяца.

> Обратите внимание, что вы выбираете порядковый номер дня недели в месяце, а не конкретную дату в месяце или номер недели (первая, вторая неделя месяца). Например, если вы выберите ячейку **Вт** в строке **Первая**, в этом случае задача будет запускаться каждый первый вторник каждого нового месяца.

Вы можете выбрать несколько дней недели.

При загрузке обновлений в хранилище

Эта задача запускается после загрузки обновлений в хранилище. Например, вам может понадобиться это расписание для задачи *Обновление*.

По завершении другой задачи

Текущая задача будет запущена после завершения другой задачи. Этот параметр работает, только если обе задачи назначены одним и тем же устройствам. Например, вы можете запустить задачу *Управление устройствами* с помощью параметра **Включить устройство** и после ее завершения запустить задачу *Поиск вирусов*, как запускающую задачу.

Вам нужно выбрать запускающую задачу из таблицы и статус, с которым эта задача должна завершиться (**Завершена успешно** или **Сбой**).

При необходимости вы можете искать, сортировать и фильтровать задачи в таблице следующим образом:

- Введите название задачи в поле поиска, чтобы выполнить поиск задачи по названию.
- Нажмите на значок сортировки, чтобы отсортировать задачи по имени.

  По умолчанию задачи отсортированы в алфавитном порядке по возрастанию.
- Нажмите на значок фильтра и в открывшемся окне отфильтруйте задачи по группам, после чего нажмите на кнопку **Применить**.

Если вы создаете для управляемого приложения задачу, расписание которой можно поставить на паузу, доступны следующие настройки расписания такой задачи:

- **Время окончания**

  Выполнение расписания задачи прекратится, начиная с 00 часов 00 минут указанной даты. При этом если в момент прекращения расписания задачи сама задача еще выполняется, ее выполнение не прерывается.

  Например, существует задача, которая запускается в 23:00 ежедневно. Вы указываете, что 1 января расписание этой задачи будет прекращено. 31 декабря задача запускается в 23:00, а 1 января в 0:00 ее расписание ставится на паузу: задача продолжает выполняться до завершения, а 1 января в 23:00 расписание больше не запускается.

  Параметр доступен для всех типов расписания, кроме **Вручную** и **Один раз**.
- **Приостановить выполнение задачи**

  Если параметр включен, вы можете задать временной интервал, в течение которого выполнение задачи, запущенной ранее по расписанию, будет приостановлено. Например, с 10:00 до 11:00.

  Это может понадобиться в период наиболее активного использования устройства чтобы снизить влияние управляемого приложения (например, Kaspersky Endpoint Security) на производительность.

  Параметр доступен для всех типов расписания.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию. Для расписания **Вручную**, **Один раз** и **Немедленно** задачи выполняются только на тех клиентских устройствах, которые видны в сети. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **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.

  По умолчанию параметр включен.

- **Использовать автоматическую случайную задержку запуска задачи в интервале**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

- Окно Выбор устройств, которым будет назначена задача:

  Выбрать устройства, обнаруженные в сети Сервером администрирования

  В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

  Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

  Задать адреса устройств вручную или импортировать из списка

  Вы можете задавать DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

  Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, 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 было установлено и запущено приложение, выполняющее эту задачу.

  По умолчанию выбран этот вариант.

  Задать учетную запись

  В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.

  Учетная запись.

  Учетная запись, от имени которой будет запускаться задача.

  Пароль

  Пароль учетной записи, от имени которой будет запускаться задача.

Параметры, заданные после создания задачи

Вы можете задать следующие параметры только после создания задачи.

- Параметры групповой задачи:

  Распространить на подгруппы

  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.

Распространить 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 **Распространить на подгруппы** включен.

По умолчанию параметр выключен.

- Дополнительные параметры расписания:

  Включать устройства перед запуском задачи функцией Wake-on-LAN

  Если флажок установлен, операционная система на устройстве будет загружаться за указанное время до начала выполнения задачи. Время, заданное по умолчанию, – 5 минут.

  Включите этот параметр, если вы хотите, чтобы задача выполнялась на всех клиентских устройствах из области задач, включая те устройства, которые выключены, когда задача вот-вот начнется.

  Если нужно, чтобы устройства автоматически выключались после выполнения задачи, включите параметр **Выключать устройства после выполнения задачи**. Параметр находится в этом же окне.

  По умолчанию параметр выключен.

  Выключать устройства после выполнения задачи

  Например, вы можете включить этот параметр для задачи установки обновлений, которая устанавливает обновления на клиентские устройства каждую пятницу после рабочего времени, а затем выключает эти устройства на выходные.

  По умолчанию параметр выключен.

  Остановить, если задача выполняется дольше

  По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

  Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

  По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

- Параметры уведомления:

  - Блок **Сохранять информацию о результатах**:

    Хранить в базе данных Сервера администрирования в течение (сут)

    События приложения, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся на Сервере администрирования в течение указанного количества дней. По истечении этого периода информация удаляется с Сервера администрирования.

    По умолчанию параметр включен.

    Хранить в журнале событий ОС на устройстве

    События приложения, связанные с выполнением задачи, хранятся локально в системном журнале событий каждого клиентского устройства.

    По умолчанию параметр выключен.

Хранить в журнале событий ОС на Сервере администрирования

События приложения, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся централизованно в системном журнале событий операционной системы Сервера администрирования.

По умолчанию параметр выключен.

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**.

Экспорт задачи

Kaspersky Security Center Linux позволяет сохранить задачу и ее параметры в файл KLT. Вы можете использовать файл KLT для импорта сохраненной задачи как в Kaspersky Security Center Windows, так и в Kaspersky Security Center Linux.

Чтобы экспортировать задачу:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Установите флажок рядом с задачей, которую вы хотите экспортировать.

   Невозможно экспортировать несколько задач одновременно. Если вы выберете несколько задач, кнопка **Экспортировать** будет неактивна. Задачи Сервера администрирования также недоступны для экспорта.
3. Нажмите на кнопку **Экспортировать**.
4. В открывшемся окне **Сохранить как** укажите имя файла задачи и путь. Нажмите на кнопку **Сохранить**.

   Окно **Сохранить как** отображается только в том случае, если вы используете Google Chrome, Microsoft Edge или Opera. Если вы используете другой браузер, файл задачи автоматически сохраняется в папку **Загрузки**.

Импорт задачи

Kaspersky Security Center Linux позволяет импортировать задачу из файла KLT. Файл KLT содержит экспортированную задачу и ее параметры.

Для корректного импорта задачи приложения "Лаборатории Касперского" нужно установить соответствующий плагин управления.

Чтобы импортировать задачу:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Импортировать**.
3. Нажмите на кнопку **Обзор**, чтобы выбрать файл задачи, которую вы хотите импортировать.
4. В открывшемся окне укажите путь к файлу KLT задачи и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл задачи.

   Начнется обработка задачи.
5. После того как задача будет успешно обработана, выберите устройства, которым вы хотите назначить задачу. Для этого выберите один из следующих параметров:

Назначить задачу группе администрирования

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 определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

Назначить задачу выборке устройств

Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

6. Укажите область действия задачи.

7. Нажмите на кнопку **Завершить**, чтобы завершить задачу импорта.

Появится уведомление с результатами импорта. Если задача успешно импортирована, вы можете перейти по ссылке **Подробнее** для просмотра свойств задачи.

После успешного импорта задача отображается в списке задач. Параметры задачи и расписание также импортируются. Задача будет запущена в соответствии с расписанием.

Если имя новой импортированной задачи идентично имени существующей задачи, имя импортированной задачи расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Запуск мастера изменения паролей задач

Для не-локальной задачи, можно указать учетную запись, с правами которой будет запускаться задача. Учетную запись можно указать во время создания задачи или в свойствах существующей задачи. Если указанная учетная запись используется в соответствии с правилами безопасности, установленными в организации, эти правила могут требовать периодического изменения пароля учетной записи. После истечения срока действия пароля учетной записи и задания нового пароля, задача не будет запускаться до тех пор, пока вы не укажете новый действующий пароль в свойствах задачи.

Мастер изменения паролей задач позволяет автоматически заменить старый пароль на новый во всех задачах, в которых указана учетная запись. Вы также можете изменить пароль вручную в свойствах каждой задачи.

Чтобы запустить мастер изменения паролей задач

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Управление учетными данными учетной записи для запуска задач**.

Следуйте далее указаниям мастера.

Шаг 1. Выбор учетных данных

Укажите новые учетные данные, которые в настоящее время действительны в вашей системе. При переходе на следующий шаг мастера, Kaspersky Security Center Linux проверяет, совпадает ли имя указанной учетной записи с именем учетной записи в свойствах каждой не-локальной задачи. Если имена учетных записей совпадают, пароль в свойствах задачи автоматически меняется на новый.

Чтобы указать новую учетную запись, выберите один из вариантов:

Использовать текущую учетную запись

Мастер использует имя учетной записи, под которой вы в настоящее время вошли в Kaspersky Security Center Web Console. Вручную укажите пароль учетной записи в поле **Актуальный пароль для использования в задачах**.

Указать другую учетную запись

Укажите имя учетной записи, под которой должны запускаться задачи. Укажите пароль учетной записи в поле **Актуальный пароль для использования в задачах**.

При заполнении поля **Предыдущий пароль (необязательно; если вы хотите заменить его на текущий)** Kaspersky Security Center Linux 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 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.

Чтобы посмотреть результаты выполнения задачи:

в окне свойств задачи перейдите на вкладку **Результаты.**

Чтобы просмотреть результаты задачи для подчиненного Сервера администрирования:

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.
3. Нажмите на **Статистика подчиненного Сервера**.
4. Выберите подчиненный Сервер, для которого вы хотите отобразить окно **Результаты выполнения задачи**.

Теги приложений

В этом разделе описаны теги приложений, приведены инструкции по их созданию и изменению, а также по назначению тегов сторонним приложениям.

Теги приложений

Kaspersky Security Center Linux позволяет назначать теги приложениям из реестра приложений. Тег представляет собой метку приложения, которую можно использовать для группировки и поиска приложений. Назначенный приложению 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 приложений

Чтобы создать тег приложения:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Теги приложений**.
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 приложения.

Изменение тегов приложений

Чтобы изменить тег приложения:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Теги приложений**.
2. Установите флажок рядом с тегом, который вы хотите переименовать, и нажмите на кнопку **Изменить**.

   Откроется окно свойств тега.
3. Измените тег.
4. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Обновленный тег появится в списке тегов приложений.

Назначение тегов приложениям

Чтобы назначить приложению теги:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Реестр приложений**.
2. Выберите приложение, для которого требуется назначить теги.

3. Выберите вкладку **Теги**.

   На вкладке появятся все теги приложений, существующие на Сервере администрирования. Теги, назначенные выбранному приложению, отмечены флажками в столбце **Назначенный тег**.

4. Установите флажки в столбце **Назначенный тег** для тегов, которые требуется назначить.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Теги назначены приложению.

Снятие назначенных тегов с приложений

Чтобы снять теги с приложения:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Реестр приложений**.

2. Выберите приложение, с которого требуется снять теги.

3. Выберите вкладку **Теги**.

   На вкладке появятся все теги приложений, существующие на Сервере администрирования. Теги, назначенные выбранному приложению, отмечены флажками в столбце **Назначенный тег**.

4. Снимите флажки в столбце **Назначенный тег** для тегов, которые требуется снять.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Теги будут сняты с приложения.

Снятые с приложений теги не удаляются. При необходимости их можно удалить вручную.

Удаление тегов приложений

Чтобы удалить тег приложения:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Теги приложений**.

2. В списке выберите теги приложения, которые вы хотите удалить.

3. Нажмите на кнопку **Удалить**.

4. В появившемся окне нажмите на кнопку **ОК**.

Выбранный тег приложения удален. Удаленный тег автоматически снимается со всех приложений, которым он был назначен.

Использование утилиты klscflag для открытия порта 13291

Вы можете автоматизировать работу Kaspersky Security Center Linux с помощью утилиты klakaut. Утилита klakaut и справочная система для нее расположены в папке установки Kaspersky Security Center Linux. 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 Linux, 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`.

Регистрация приложения Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center Web Console

Чтобы начать работу с приложением Kaspersky Industrial CyberSecurity for Networks через Kaspersky Security Center Web Console, необходимо предварительно зарегистрировать его в Kaspersky Security Center Web Console.

Чтобы зарегистрировать приложение Kaspersky Industrial CyberSecurity for Networks:

1. Убедитесь, что сделано следующее:

   - Вы загрузили и установили веб-плагин Kaspersky Industrial CyberSecurity for Networks.

     Можно сделать это позже, ожидая синхронизацию Сервера Kaspersky Industrial CyberSecurity for Networks с Сервером администрирования. После загрузки и установки плагина в главном меню Kaspersky Security Center Web Console отображается раздел **KICS for Networks**.

   - В веб-интерфейсе Kaspersky Industrial CyberSecurity for Networks настраивается и включается взаимодействие с Kaspersky Security Center Linux. Подробную информацию см. в справке Kaspersky Industrial CyberSecurity for Networks.

2. Переместите устройство, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks, из группы Нераспределенные устройства в группу Управляемые устройства:

   a. В главном окне приложения перейдите в раздел **Управление активами** → **Нераспределенные устройства**.

   b. Установите флажок рядом с устройством, на котором установлен Kaspersky Industrial CyberSecurity for Networks Server.

   c. Нажмите на кнопку **Переместить в группу**.

   d. В иерархии групп администрирования установите флажок рядом с группой **Управляемые устройства**.

   e. Нажмите на кнопку **Переместить**.

3. Откройте окно свойств устройства, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks.

4. На странице свойств устройства в разделе **Общие** выберите параметр **Не разрывать соединение с Сервером администрирования**, а затем нажмите на кнопку **Сохранить**.

5. В окне свойств устройства выберите раздел **Приложения**.

6. В разделе **Приложения** выберите Агент администрирования Kaspersky Security Center Network.

7. Если текущий статус приложения *Остановлено*, подождите, пока он не изменится на *Выполняется*.

   Это может занять до 15 минут. Если вы еще не установили веб-плагин Kaspersky Industrial CyberSecurity for Networks, вы можете сделать это сейчас.

8. Если вы хотите просматривать статистику работы Kaspersky Industrial CyberSecurity for Networks, вы можете добавить виджеты в панель управления. Чтобы добавить виджеты, выполните следующее:

   a. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга**.

   b. В панели управления нажмите на кнопку **Добавить или восстановить виджет**.

   c. В появившемся виджете нажмите на кнопку **Другое**.

d. Выберите виджет, который вы хотите добавить.

- Карта размещения KICS for Networks
- Информация о Серверах KICS for Networks
- Актуальные события KICS for Networks
- Устройства, требующие внимания в KICS for Networks
- Критические события KICS for Networks
- Статусы KICS for Networks

9. Чтобы перейти в веб-интерфейс Kaspersky Industrial CyberSecurity for Networks, выполните следующие действия:

a. В главном окне приложения перейдите в раздел **KICS for Networks** → **Поиск**.

b. Нажмите на кнопку **Найти события или устройства**.

c. В открывшемся окне **Параметры запроса** нажмите на поле **Сервер**.

d. В раскрывающемся списке серверов, интегрированных с Kaspersky Security Center Linux, выберите Сервер Kaspersky Industrial CyberSecurity for Networks и нажмите на кнопку **Найти**.

e. Перейдите по ссылке **Перейти на Сервер** рядом с названием Сервера Kaspersky Industrial CyberSecurity for Networks.

Откроется страница входа в Kaspersky Industrial CyberSecurity for Networks.

Для входа в веб-интерфейс Kaspersky Industrial CyberSecurity for Networks вам необходимо ввести учетные данные пользователя приложения.

Управление пользователями и ролями пользователей

В этом разделе описана работа с пользователями и ролями пользователей, а также приведены инструкции по их созданию и изменению, назначению пользователям ролей и групп и связи профилей политики с ролями.

Об учетных записях пользователей

Kaspersky Security Center Linux позволяет управлять учетными записями пользователей и группами безопасности. Приложение поддерживает три типа учетных записей:

- Учетные записи сотрудников организации. Сервер администрирования получает данные об учетных записях этих доменных пользователей при опросе контроллеров доменов организации.
- Учетные записи локальных пользователей. Локальные учетные записи управляемых устройств, а также локальные учетные записи устройства, на котором установлен Сервер администрирования.
- Учетные записи внутренних пользователей Kaspersky Security Center Linux. Вы можете создавать учетные записи внутренних пользователей. Эти учетные записи используются только в Kaspersky Security Center Linux.

Учетные записи локальных пользователей и локальная группа kladmins в операционной системе Linux не могут быть использованы для доступа к Kaspersky Security Center Web Console в Kaspersky Security Center Linux. Группа kladmins может содержать только учетные записи, которые используются для запуска служб Kaspersky Security Center Linux. Использование учетных записей сотрудников организации для входа становится доступно после настройки доменной аутентификации.

Чтобы просмотреть таблицы учетных записей пользователей и групп безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы**.
2. Перейдите на вкладку **Пользователи** или **Группы**.

Откроется таблица пользователей или групп безопасности. Если вы хотите просмотреть таблицу только с учетными записями внутренних пользователей или групп, установите в фильтре **Тип учетной записи** критерий **Внутренний** или **Локальный**.

Если таблица пользователей содержит более 50 000 пользователей, отображаются только первые 50 000 пользователей, остальные пользователи не отображаются.

О ролях пользователей

Роль пользователя (далее также *роль*) это объект, содержащий набор прав и разрешений. Роль может быть связана с параметрами приложениями "Лаборатории Касперского", которые установлены на устройстве пользователя. Вы можете назначить роль набору пользователей или набору групп безопасности на любом уровне иерархии групп администрирования, Серверов администрирования либо на уровне конкретных объектов.

Если вы управляете устройствами с помощью иерархии Серверов администрирования, в которую входят виртуальные Серверы администрирования, обратите внимание, что вы можете создавать, изменять и удалять пользовательские роли только на физическом Сервере администрирования. Затем вы можете распространить пользовательские роли на подчиненные Серверы администрирования, в том числе виртуальные Серверы.

Вы можете связывать роли с профилями политик. Если пользователю назначена роль, этот пользователь получает параметры безопасности, требуемые для выполнения служебных обязанностей.

Роль пользователя может быть связана с устройствами пользователей заданной группы администрирования.

Область роли пользователя

Область роли пользователя – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

Преимущество использования ролей

Преимущество использования ролей заключается в том, что вам не нужно указывать параметры безопасности для каждого управляемого устройства или для каждого из пользователей отдельно. Количество пользователей и устройств в компании может быть большим, но количество различных служебных обязанностей, требующих разных параметров безопасности, значительно меньше.

Отличия от использования профилей политики

Профили политики – это свойства политики, созданной для каждого приложения "Лаборатории Касперского" отдельно. Роль связана со многими профилями политики, которые созданы для разных приложений. Таким образом, роль – это метод объединения параметров для определенного типа пользователя.

Настройка прав доступа к функциям приложения. Управление доступом на основе ролей

Kaspersky Security Center Linux предоставляет доступ на основе ролей к функциям Kaspersky Security Center Linux и к функциям управляемых приложений "Лаборатории Касперского".

Вы можете настроить права доступа к функциям приложения 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 приложению. Права доступа в роли настраивают в соответствии с типовыми задачами и служебными обязанностями пользователей.

Ролям пользователя можно давать названия, соответствующие их назначению. В приложение 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 приложения

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**, **Запись** и **Выполнение** применимы к любой задаче, отчету или параметрам. В дополнение к этим правам у пользователя должно быть право **Выполнение операций с выборками устройств** для управления задачами, отчетами или изменения параметров выборок устройств.

> Все задачи, отчеты, параметры и инсталляционные пакеты, отсутствующие в таблице, относятся к области **Общие функции: Базовая функциональность**.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
Общие функции: **Управление группами администрирования**	**Запись.**	• Добавление устройства в группу администрирования: **Запись**. • Удаление устройства из состава группы администрирования: **Запись**. • Добавление группы администрирования в другую группу администрирования: **Запись**. • Удаление группы администрирования из другой группы администрирования: **Запись**.	Отсутствует.	Отсутствует.	Отс

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
Общие функции: **Доступ к объектам независимо от их списков ACL**	**Чтение.**	Получение доступа на чтение ко всем объектам: **Чтение**.	Отсутствует.	Отсутствует.	Фун обла **фун** **к об** **неза** **спи** пред для поль пред прав этой фун обла полу дост ко в Реко пред прав огра круг поль кото нужн выпо слу обяз Дос пред неза друг если запр дост опре объ
Общие функции: **Базовая функциональность**	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Правила перемещения устройства (создание, изменение или удаление) для виртуального Сервера: **Запись**, **Выполнение действий над выборками устройств**. • Получение мобильного протокола (LWNGT) пользовательского сертификата: **Чтение**. • Установка мобильного протокола (LWNGT) пользовательского сертификата: **Запись**. • Получить список сетей, определенных NLA: **Чтение**. • Добавить, изменить или удалить список сетей, определенных NLA: **Запись**. • Просмотр списка контроля доступа групп: **Чтение**.	• Загрузка обновлений в хранилище Сервера администрирования. • Рассылка отчетов. • Распространение инсталляционных пакетов. • Установка приложений на подчиненные Серверы администрирования.	• Отчет о состоянии защиты. • Отчет об угрозах. • Отчет о наиболее заражаемых устройствах. • Отчет о статусе антивирусных баз. • Отчет об ошибках. • Отчет о сетевых атаках. • Сводный отчет о приложениях для защиты почтовых систем. • Сводный отчет о приложениях для защиты рабочих станций и файловых серверов. • Сводный отчет о приложениях для защиты периметра. • Сводный отчет о типах установленных приложений. • Отчет о пользователях зараженных устройств. • Отчет об проблемах безопасности. • Отчет о событиях.	Отсу

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
		• Просмотр журнала операционной системы: **Чтение**. • Просмотр ключа восстановления для восстановления доступа к жесткому диску зашифрованному с помощью BitLocker: **Выполнить**.		• Отчет о работе точек распространения. • Отчет о подчиненных Серверах администрирования. • Отчет о событиях Контроля устройств. • Отчет об уязвимостях. • Отчет о запрещенных приложениях. • Отчет о работе Веб-Контроля. • Отчет о статусе шифрования управляемых устройств. • Отчет о статусе шифрования запоминающих устройств. • Отчет о правах доступа к зашифрованным жестким дискам. • Отчет об ошибках шифрования файлов. • Отчет о блокировании доступа к зашифрованным файлам. • Отчет об эффективных правах пользователя. • Отчет о правах.	
Общие функции: **Удаленные объекты**	• **Чтение.** • **Запись.**	• Просмотр удаленных объектов в корзине: **Чтение**. • Удаление объектов из корзины: **Запись**.	Отсутствует.	Отсутствует.	Отс
Общие функции: **Обработка событий**	• **Удаление событий.** • **Изменение параметров уведомления о событиях.** • **Изменение параметров записи событий в журнал событий.** • **Запись.**	• Изменение параметров регистрации событий: **Изменение параметров записи событий в журнал событий**. • Изменение параметров уведомления о событиях: **Изменение параметров уведомления о событиях**. • Удаление событий: **Удаление событий**.	Отсутствует.	Отсутствует.	Пара • •

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
Общие функции: **Операции с Сервером администрирования**	• **Чтение.** • **Запись.** • **Выполнение.** • **Изменение списков ACL объекта.** • **Выполнение действий над выборками устройств.**	• Изменение портов Сервера администрирования для подключения Агента администрирования: **Запись**. • Изменение портов прокси-сервера активации, запущенного на Сервере администрирования: **Запись**. • Изменение портов прокси-сервера активации для мобильных устройств, запускаемых на Сервере администрирования: **Запись**. • Изменение портов Веб-сервера для распространения автономных пакетов: **Запись**. • Изменение портов Веб-сервера для распространения iOS MDM-профилей: **Запись**. • Изменение SSL-портов Сервера администрирования для подключения с помощью Kaspersky Security Center Web Console: **Запись**. • Изменение портов Сервера администрирования для подключения мобильных устройств: **Запись**. • Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования: **Запись**. • Укажите максимальное количество событий, которое может отправлять Сервер администрирования: **Запись**. • Изменение периода, в течение которого Сервер администрирования может отправлять события: **Запись**.	• Резервное копирование данных Сервера администрирования. • Обслуживание базы данных.	Отсутствует.	Отс
Общие функции: **Развертывание приложений "Лаборатории Касперского"**	• **Управление патчами "Лаборатории Касперского".** • **Чтение.** • **Запись.**	Одобрить или отклонить установку патча: **Управление патчами "Лаборатории Касперского"**.	Отсутствует.	• Отчет об использовании лицензионных ключей виртуальным Сервером администрирования.	Инст паке "Лаб Касп

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
	• **Выполнение.** • **Выполнение действий над выборками устройств.**			• Отчет о версиях приложений "Лаборатории Касперского". • Отчет о несовместимых приложениях. • Отчет о версиях обновлений модулей приложений "Лаборатории Касперского". • Отчет о развертывании защиты.	
Общие функции: **Управление лицензионными ключами**	• **Экспорт файл ключа.** • **Запись.**	• Экспорт файл ключа: **Экспорт файл ключа.** • Изменение параметров лицензионного ключа Сервера администрирования: **Запись**.	Отсутствует.	Отсутствует.	Отс
Общие функции: **Управление отчетами**	• **Чтение.** • **Запись.**	• Создание отчетов для объектов независимо от их списков ACL: **Запись**. • Выполнять отчеты независимо от их списков ACLs: **Чтение**.	Отсутствует.	Отсутствует.	Отс
Общие функции: **Иерархия Серверов администрирования**	**Настройка иерархии Серверов администрирования**	• Добавление, обновление или удаление подчиненных Серверов администрирования: **Настройка иерархии Серверов администрирования**.	Отсутствует.	Отсутствует.	Отс
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.	Отс
Общие функции: **Виртуальные Серверы администрирования**	• **Управление виртуальными Серверами администрирования.**	• Получение списка виртуальных Серверов	Отсутствует.	Отсутствует.	Отс

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	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**.			

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
Общие функции: **Управление ключами шифрования**	**Запись.**	Импорт ключей шифрования: **Запись**.	Отсутствует.	Отсутствует.	Отс
Управление мобильными устройствами: **Общие**	• **Подключение новых устройств.** • **Отправка только информационных команд на мобильные устройства.** • **Отправка команд на мобильные устройства.** • **Управление сертификатами.** • **Чтение.** • **Запись.**	• Получение восстановленных данных службы управления ключами: **Чтение**. • Удаление сертификатов пользователей: **Управление сертификатами**. • Получение публичной части сертификата пользователя: **Чтение**. • Проверка, включена ли инфраструктура открытых ключей: **Чтение**. • Проверка учетной записи инфраструктуры открытых ключей: **Чтение**. • Получение шаблонов инфраструктуры открытых ключей: **Чтение**. • Получение шаблонов инфраструктуры открытых ключей с помощью расширенного использования ключа (EKU) сертификата: **Чтение**. • Проверка, не отозван ли сертификат инфраструктуры открытых ключей: **Чтение**. • Обновление параметров выпуска сертификатов пользователя: **Управление сертификатами**. • Получение параметров выпуска сертификатов пользователя: **Чтение**. • Получение пакетов по названию и версиям приложений: **Чтение**. • Установка или отмена сертификатов пользователя: **Управление сертификатами**. • Обновление сертификата пользователя: **Управление сертификатами**.	Отсутствует.	Отсутствует.	Отс

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
		• Установка тега для сертификата пользователя: **Управление сертификатами**. • Запуск генерации инсталляционного пакета, содержащего iOS MDM-профиль; отмена генерации инсталляционного пакета, содержащего iOS MDM-профиль: **Подключение новых устройств**.			
Управление системой: **Подключения**	• **Запуск RDP-сеансов.** • **Подключение к существующим RDP-сеансам.** • **Туннелирование.** • **Сохранение файлов с устройств на рабочем месте администратора.** • **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Создание сеанса совместного доступа к рабочему столу: **Право на создание сеанса совместного доступа к рабочему столу**. • Создание RDP-сеанса: **Подключение к существующим RDP-сеансам**. • Создание туннеля: **Туннелирование**. • Сохранение списка сетей: **Сохранение файлов с устройств на рабочем месте администратора**.	Отсутствует.	Отчет о пользователях устройства.	Отс
Управление системой: **Системное администрирование**	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Просмотр свойства патчей сторонних производителей: **Чтение**. • Изменение свойства патчей сторонних производителей: **Запись**.	• Закрытие уязвимостей. • Установка требуемых обновлений и закрытия уязвимостей.	Отчет об обновлениях ПО.	Отс
Управление системой: **Удаленное выполнение скриптов**	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	Пользователь может просматривать свойства задачи: **Чтение**. Пользователь может создать, удалить или изменить инсталляционный пакет: **Запись**. Пользователь может запустить задачу: **Запись**. На клиентских устройствах с операционной системой Linux скрипты выполняются с правами root. Пользователь может запустить задачу или запланировать ее запуск: **Выполнение**.	"Удаленное выполнение скриптов"	Отсутствует.	Отс

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
		Пользователь может запустить задачу на выбранных устройствах: **Выполнение действий над выборками устройств**.			

Предопределенные роли пользователей

Роли пользователей, назначенные пользователям Kaspersky Security Center Linux, предоставляют им набор прав доступа к функциям приложения.

Пользователям, которые были созданы на виртуальном Сервере, невозможно назначить роли на Сервере администрирования.

Вы можете использовать предопределенные роли пользователей с уже настроенным набором прав или создавать роли. При создании роли вам нужно задать область действия и назначить права доступа к функциям Kaspersky Security Center Linux. 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	Разрешены все операции по просмотру и выполнению любых созданных задач на выбранных устройствах, подключенных к Серверу администрирования через Агент администрирования с правами локального администратора (с правами root для Linux). Рекомендуется предоставлять эти права ограниченному количеству пользователей, которым они нужны для выполнения своих служебных обязанностей.
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.

Права предопределенных ролей пользователей

Роль	Описание

Администратор Сервера администрирования	Разрешает все операции в следующих функциональных областях:
	• **Общие функции**:
	  • **Базовая функциональность.**
	  • **Управление ключами шифрования.**
	  • **Обработка событий.**
	  • **Иерархия Серверов администрирования.**
	  • **Виртуальные Серверы администрирования.**
	• **Управление системой**:
	  • **Подключения.**
	  • **Инвентаризация оборудования.**
	  • **Инвентаризация приложений.**

Оператор Сервера администрирования	Предоставляет права на **Чтение** и **Выполнение** (если применимо) во всех следующих функциональных областях:
	• **Общие функции**:
	  • **Базовая функциональность.**
	  • **Управление ключами шифрования.**
	  • **Виртуальные Серверы администрирования.**
	• **Управление системой**:
	  • **Подключения.**
	  • **Инвентаризация оборудования.**
	  • **Инвентаризация приложений.**

Аудитор	Разрешает все операции в следующих функциональных областях: **Общие функции**: • **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 приложений	Разрешает все операции в следующих функциональных областях:
	• **Общие функции:**
	  • **Базовая функциональность.**
	  • **Приложения "Лаборатории Касперского".**
	  • **Управление лицензионными ключами.**
	• **Управление системой:**
	  • **Развертывание операционной системы.**
	  • **Системное администрирование.**
	  • **Удаленная установка.**
	  • **Инвентаризация приложений.**
	Предоставляет права на **Чтение** и **Выполнение** в следующей функциональной области **Базовая функциональность: Виртуальные Серверы администрирования**.

Роль	Описание

Оператор установки приложений	Предоставляет права на **Чтение** и **Выполнение** (если применимо) во всех следующих функциональных областях:
	• **Общие функции:**
	  • **Базовая функциональность.**
	  • **Развертывание приложений "Лаборатории Касперского"** (также предоставляет права на **Управление патчами "Лаборатории Касперского"** в этой же области).
	  • **Виртуальные Серверы администрирования.**
	• **Управление системой:**
	  • **Развертывание операционной системы.**
	  • **Системное администрирование.**
	  • **Удаленная установка.**
	  • **Инвентаризация приложений.**

Администратор Kaspersky Endpoint Security	Разрешает все операции в следующих функциональных областях: • **Общие функции: Базовая функциональность.** • **Общие функции: Управление ключами шифрования.** • Область **Kaspersky Endpoint Security**, включая все функции.
Оператор Kaspersky Endpoint Security	Предоставляет права на **Чтение** и **Выполнение** (если применимо) во всех следующих функциональных областях: • **Общие функции: Базовая функциональность.** • **Общие функции: Управление ключами шифрования.** • Область **Kaspersky Endpoint Security**, включая все функции.
Главный администратор	Разрешает все операции в функциональных областях, *за исключением* следующих областей: **Общие функции**: • **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.**
	  • **Управление ключами шифрования.**
	  • **Операции с Сервером администрирования.**
	  • **Теги устройств.**
	  • **Приложения "Лаборатории Касперского".**
	  • **Интеграция приложений.**
	  • **Виртуальные Серверы администрирования.**
	• Функциональная область **Управление мобильными устройствами**, включая все функции.
	• Функциональная область **Управление системой**, включая все функции.
	• Область **Kaspersky Endpoint Security**, включая все функции.

Администратор управления мобильными устройствами	Разрешает все операции в следующих функциональных областях: • **Общие функции: Базовая функциональность.** • Функциональная область **Управление мобильными устройствами**, включая все функции. Предоставляет право **Экспортировать файл ключа** в области **Общие функции: Управление лицензионными ключами**. Предоставляет право на **Чтение** в области **Управление системой: Системное администрирование**.
Оператор управления мобильными устройствами	Предоставляет права на **Чтение** и **Выполнение** в области **Общие функции: Базовая функциональность**. Предоставляет права на **Чтение** и **Отправка только информационных команд на мобильные устройства** в области **Управление мобильными устройствами**: • **Общие.** • **Self Service Portal.**

Роль	Описание
Специалист по безопасности	Разрешает все операции в следующих функциональных областях: **Общие функции**: • **Доступ к объектам независимо от их списков ACL.** • **Управление отчетами.** Предоставляет следующие права в функциональной области **Управления системой: Подключения**: **Чтение**, **Запись**, **Выполнение**, **Сохранение файлов с устройств на рабочем месте администратора** и **Выполнение операций с выборками устройств**. 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**.
Контролер	Предоставляет права на **Чтение** в области **Общие функции**: **Доступ к объектам независимо от их списков ACL** и **Общие функции**: функциональная область **Управление отчетами**. Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации.
Администратор Системного администрирования	Разрешает все операции в области **Общие функции**: **Базовая функциональность** и **Управление системой** (включая все функции, *кроме* области **Удаленное выполнение скриптов**).
Оператор Системного администрирования	Предоставляет права на **Чтение** и **Выполнение** (если применимо) в области **Общие функции**: **Базовая функциональность** и **Управление системой** (включая все функции, *кроме* области **Удаленное выполнение скриптов**).

Назначение прав доступа к набору объектов

В дополнение к назначению прав доступа на уровне сервера, вы можете настроить доступ к конкретным объектам, например, к требуемой задаче. Приложение позволяет указать права доступа к следующим типам объектов:

- Группы администрирования
- Задачи
- Отчеты
- Выборки устройств
- Выборки событий

Чтобы назначить права доступа к конкретному объекту:

1. В зависимости от типа объекта в главном меню перейдите в соответствующий раздел:
   - **Управление активами → Иерархия групп**.
   - **Задачи**.
   - **Мониторинг → Отчеты**.
   - **Управление активами → Выборки устройств**.
   - **Мониторинг → Выборки событий**.
2. Откройте свойства объекта, к которому вы хотите настроить права доступа.

   Чтобы открыть окно свойств группы администрирования или задачи, нажмите на название объекта. Свойства других объектов можно открыть с помощью кнопки в панели инструментов.

3. В окне свойств откройте раздел **Права доступа**.

   Откроется список пользователей. Перечисленные пользователи и группы безопасности имеют права доступа к объекту. Если вы используете иерархию групп администрирования или Серверов, список и права доступа по умолчанию наследуются от родительской группы администрирования или главного Сервера.

4. Чтобы иметь возможность изменять список, включите параметр **Использовать права пользователей**.

5. Настройте права доступа:

   - Используйте кнопки **Добавить** и **Удалить** для изменения списка.
   - Укажите права доступа для пользователя или группы безопасности. Выполните одно из следующих действий:
     - Если вы хотите указать права доступа вручную, выберите пользователя или группу безопасности, нажмите на кнопку **Права доступа** и укажите права доступа.
     - Если вы хотите назначить пользовательскую роль пользователю или группе безопасности, выберите пользователя или группу безопасности, нажмите на кнопку **Роли** и выберите роль для назначения.

6. Нажмите на кнопку **Сохранить**.

Права доступа к объекту настроены.

Назначение прав пользователям или группам безопасности

Вы можете назначить права доступа пользователям или группам безопасности, чтобы использовать различные возможности Сервера администрирования, например Kaspersky Endpoint Security для Linux.

Чтобы назначить права доступа пользователю или группе безопасности:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Права доступа** установите флажок рядом с именем пользователя или группы безопасности, которым нужно назначить права, а затем нажмите на кнопку **Права доступа**.

   Вы не можете выбрать несколько пользователей или групп безопасности одновременно. Если вы выберете более одного объекта, кнопка **Права доступа** будет неактивна.

3. Настройте набор прав для пользователя или группы:

   a. Разверните узел с функциями Сервера администрирования или другого приложения "Лаборатории Касперского".

   b. Установите флажок **Разрешить** или **Запретить** рядом с нужной функцией или правом доступа.

      Пример 1: Установите флажок **Разрешить** рядом с узлом **Интеграции приложения**, чтобы предоставить пользователю или группе все доступные права доступа к функции интеграции приложения (**Чтение**, **Запись** и **Выполнение**).

Пример 2: Разверните узел **Управление ключами шифрования** и установите флажок **Разрешить** рядом с разрешением **Запись**, чтобы предоставить пользователю или группе право доступа на **Запись** к функции управления ключами шифрования.

4. После настройки набора прав доступа нажмите на кнопку **ОК**.

Набор прав для пользователя или группа пользователей настроен.

Права Сервера администрирования (или группы администрирования) разделены на следующие области:

- Общие функции:
  - Управление группами администрирования
  - Доступ к объектам независимо от их списков ACL
  - Базовая функциональность
  - Удаленные объекты
  - Управление ключами шифрования
  - Обработка событий
  - Операции с Сервером администрирования (только в окне свойств Сервера администрирования)
  - Теги устройств
  - Развертывание приложений "Лаборатории Касперского"
  - Управление лицензионными ключами
  - Интеграция приложения
  - Управление отчетами
  - Иерархия Серверов администрирования
  - Права пользователей
  - Виртуальные Серверы администрирования
- Управление мобильными устройствами:
  - Общие
  - Self Service Portal
- Управление системой:
  - Подключения
  - Удаленное выполнение скриптов
  - Инвентаризация оборудования

- Network Access Control
- Развертывание ОС
- Системное администрирование
- Удаленная установка
- Инвентаризация приложений

Если для права не выбрано ни **Разрешить**, ни **Запретить**, оно считается *неопределенным*: право отклоняется до тех пор, пока оно не будет явно отклонено или разрешено для пользователя.

Права пользователей являются суммой следующего:

- собственных прав пользователя;
- прав всех ролей, назначенных пользователю;
- прав всех групп безопасности, в которые входит пользователь;
- прав всех ролей, назначенных группам, в которые входит пользователь.

Если хотя бы в одном наборе прав есть запрещенное право (для права установлен флажок **Запретить**), тогда для пользователя это право запрещено, даже если в других наборах прав оно разрешено или не определено.

Также вы можете добавить пользователей и группы безопасности в область пользовательской роли, чтобы использовать различные возможности Сервера 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.

Добавление учетной записи внутреннего пользователя

Если вы хотите добавить учетную запись пользователя, убедитесь, что у вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области Общие функции: Права пользователей.

Чтобы добавить новую учетную запись пользователя Kaspersky Security Center Linux:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Добавить пользователя** укажите параметры нового пользователя:
   - **Имя**.
   - **Пароль** для подключения пользователя к Kaspersky Security Center Linux.

Пароль должен соответствовать следующим правилам:

- Длина пароля должна быть от 8 до 256 символов.
- Пароль должен содержать символы как минимум трех групп из 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 "@", если "." расположена перед "@".

Чтобы посмотреть введенный пароль, нажмите на кнопку .

Вы можете включить параметр **Пользователю нужно сменить пароль при первом входе**, чтобы принудительно изменить пароль при первой аутентификации пользователя.

4. Сохраните изменения для завершения создания учетной записи пользователя.

Учетная запись пользователей добавлена в список пользователей.

Чтобы войти в систему с помощью созданной внутренней учетной записи пользователя в Kaspersky Security Center Web Console, вам нужно назначить этой учетной записи роль. Прежде чем войти в приложение убедитесь, что у внутренней учетной записи пользователя есть роль. Иначе возникнет ошибка.

Создание группы безопасности

Чтобы создать группу безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Группы**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Создать группу безопасности** укажите следующие параметры новой группы безопасности:
   - **Имя группы**
   - **Описание**
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Группа безопасности добавлена в список групп.

Изменение учетной записи внутреннего пользователя

Если вы хотите изменить учетную запись пользователя, убедитесь, что у вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области Общие функции: Права пользователей.

Чтобы изменить учетную запись внутреннего пользователя Kaspersky Security Center Linux:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Выберите учетную запись пользователя, которую требуется изменить.
3. В открывшемся окне на вкладке **Общие** измените параметры учетной записи пользователя:
   - **Учетная запись пользователя**

     При необходимости переведите переключатель в положение **Неактивная**, чтобы запретить пользователю подключаться к приложению. Например, можно отключить учетную запись после того, как сотрудник увольняется из компании.
   - Описание
   - **Полное имя**
   - **Адрес электронной почты**
   - **Основной телефон**
   - **Пароль**

     При необходимости вы можете установить новый пароль для подключения пользователя к Kaspersky Security Center Linux следующим образом:

     a. Нажмите на кнопку **Изменение пароля** и установите новый пароль для учетной записи пользователя.

     Пароль должен соответствовать следующим правилам:

     - Длина пароля должна быть от 8 до 256 символов.
     - Пароль должен содержать символы как минимум трех групп из 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 "@", если "." расположена перед "@".

Чтобы посмотреть введенный пароль, нажмите на кнопку .

b. При необходимости включите параметр **Пользователю нужно сменить пароль при первом входе**, чтобы принудительно изменить пароль при следующей аутентификации пользователя.

c. Если учетная запись пользователя защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите учетные данные учетной записи, у которой есть право Изменение списков управления доступом объектов в функциональной области Общие функции: Права пользователей.

4. На вкладке **Двухфакторная аутентификация** вы можете указать параметры безопасности для этой учетной записи.

5. На вкладке **Группы** можно добавить пользователя или группу безопасности.

6. На вкладке **Устройства** можно назначить устройства пользователю.

7. На вкладке **Роли** можно назначить роль пользователю.

8. Сохраните изменения для завершения изменения учетной записи пользователя.

Измененная учетная запись пользователя отобразится в списке пользователей.

Изменение группы безопасности

Чтобы изменить группу безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Группы**.

2. Выберите группу безопасности, которую требуется изменить.

3. В открывшемся окне измените параметры группы безопасности:

- На вкладке **Общие** можно изменить параметры **Имя** и **Описание**. Эти параметры доступны только для внутренних групп безопасности.
- На вкладке **Пользователи** можно добавить пользователей в группу безопасности. Эти параметры доступны только для внутренних пользователей и внутренних групп безопасности.
- На вкладке **Роли** можно назначить роль группе безопасности.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Изменения применены к группе безопасности.

Назначение роли пользователю или группе безопасности

Чтобы назначить роли пользователю или группе безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи** или **Группы**.

2. Выберите имя пользователя или группы безопасности, которой нужно назначить роль.

   Можно выбрать несколько имен.

3. В меню нажмите на кнопку **Назначить роль**.

   Будет запущен мастер назначения роли.

4. Следуйте инструкциям мастера: выберите роль, которую вы хотите назначить выбранным пользователям или группам безопасности, а затем выберите область применения роли.

   Область роли пользователя – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

В результате роль с набором прав для работы с Сервером администрирования будет назначена пользователю (или пользователям, или группе безопасности). В списке пользователей или групп безопасности отображается флажок в столбце **Имеет назначенные роли**.

Добавление учетных записей пользователей во внутреннюю группу безопасности

Учетные записи внутренних пользователей можно добавлять только во внутреннюю группу безопасности.

Чтобы добавить учетные записи пользователей в группу безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.

2. Установите флажки напротив учетных записей пользователей, которые требуется добавить в группу безопасности.

3. Нажмите на кнопку **Назначить группу**.

4. В открывшемся окне **Назначить группу** выберите группу безопасности, в которую требуется добавить учетные записи пользователей.

5. Нажмите на кнопку **Сохранить**.

Учетные записи пользователей добавлены в группу безопасности. Также можно добавить внутренних пользователей в группу безопасности, используя параметры группы.

Назначение пользователя владельцем устройства

Информацию о назначении пользователя владельцем мобильного устройства см. в справке Kaspersky Secure Mobility Management.

Чтобы назначить пользователя владельцем устройства:

1. Если вы хотите назначить владельца устройства, подключенного к виртуальному Серверу администрирования, сначала переключитесь на виртуальный Сервер администрирования:

   a. В главном меню нажмите на значок шеврона (›) справа от текущего имени Сервера администрирования.

   b. Выберите требуемый Сервер администрирования.

2. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.

   Откроется список пользователей. Если вы в данный момент подключены к виртуальному Серверу администрирования, в список входят пользователи текущего виртуального Сервера администрирования и главного Сервера администрирования.

3. Нажмите на учетную запись пользователя, которую требуется назначить в качестве владельца устройству.

4. В открывшемся окне свойств пользователя выберите вкладку **Устройства**.

5. Нажмите на кнопку **Добавить**.

6. Из списка устройств выберите устройство, которое вы хотите назначить пользователю.

7. Нажмите на кнопку **OK**.

Выбранное устройство добавляется в список устройств, назначенных пользователю.

Также можно выполнить эту операцию в группе **Управление активами** → **Управляемые устройства**, выбрав имя устройства, которое вы хотите назначить, и перейдя по ссылке **Сменить владельца устройства**.

Назначение пользователя владельцем устройства при установке Агента администрирования

Чтобы назначить пользователя владельцем устройства при установке Агента администрирования с помощью инсталляционного пакета, добавьте в параметры инсталляционного пакета Агента администрирования переменные, указанные в таблице ниже.

Имя переменной	Обязательная	Описание	Возможные значения
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Нет	Позволяет запустить утилиту для регистрации пользователя в качестве владельца устройства после установки Агента администрирования. Если выключено, то регистрация в качестве владельца устройства недоступна для пользователя.	1 – утилита для регистрации пользователя в качестве владельца устройства запустится после установки Агента администрирования. Другое – утилита недоступна.
KLNAGENT_DEVICEOWNER_LOGIN	Нет Да, если ввести пароль	Содержит учетную запись пользователя, который будет зарегистрирован как владелец устройства.	Учетная запись пользователя, который указан в списке пользователей в Kaspersky Security Center Linux.
KLNAGENT_DEVICEOWNER_PASSWORD	Нет Да, если ввести учетную запись	Содержит зашифрованный пароль пользователя, который будет зарегистрирован как владелец устройства.	Пароль пользователя.

Агент администрирования расшифрует указанные учетную запись и пароль при установке Kaspersky Security Center Linux, и пользователь будет зарегистрирован как владелец устройства.

Вы также можете назначить пользователя владельцем устройства при установке Агента администрирования в тихом режиме с файлом ответов.

Чтобы назначить пользователя владельцем устройства при установке Агента администрирования в тихом режиме с файлом ответов:

1. Добавьте параметр KLNAGENT_DEVICEOWNER_REGISTRATION_START в файл ответов и установите для него значение 1.

   Утилита для регистрации пользователя в качестве владельца устройства запустится после установки Агента администрирования.

2. Введите учетную запись и пароль в командной строке на клиентском устройстве.

   Пользователь назначен владельцем устройства.

Если пользователь входит во внутреннюю группу безопасности, учетная запись должна содержать имя пользователя.

Если пользователь входит в группу безопасности Active Directory, учетная запись должна содержать имя пользователя и имя домена.

Необходимо ввести временный одноразовый пароль (TOTP) из приложения для двухфакторной аутентификации.

Назначение пользователя владельцем устройства Linux после установки Агента администрирования

Чтобы разрешить пользователю зарегистрироваться в качестве владельца устройства Linux:

1. В Kaspersky Security Center Web Console перейдите в раздел **Управление программным обеспечением → Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов.

2. Нажмите на инсталляционный пакет Агента администрирования.

   Отобразится окно свойств инсталляционного пакета.

3. В открывшемся окне свойств инсталляционного пакета перейдите на вкладку **Параметры** → **Дополнительно**.

4. В разделе **Регистрация пользователя в качестве владельца устройства (только для Linux)** включите параметр **Разрешить запуск утилиты регистрации пользователя после установки Агента администрирования** и нажмите на кнопку **Сохранить**.

Утилиту для регистрации пользователя в качестве владельца устройства можно запустить из командной строки на клиентском устройстве.

Чтобы зарегистрировать пользователя в качестве владельца устройства Linux на клиентском устройстве:

1. Выполните следующую команду в командной строке на клиентском устройстве:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner
   ```

2. Если потребуется, введите учетную запись и пароль.

   Если учетная запись и пароль включены в файл ответов или инсталляционный пакет Агента администрирования, выполните следующую команду в командной строке на клиентском устройстве:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended
   ```

Если пользователь входит во внутреннюю группу безопасности, учетная запись должна содержать имя пользователя.

Если пользователь входит в группу безопасности Active Directory, учетная запись должна содержать имя пользователя и имя домена.

Необходимо ввести временный одноразовый пароль (TOTP) из приложения для двухфакторной аутентификации.

Пользователь зарегистрирован как владелец устройства.

Отмена назначения пользователя владельцем устройства

Чтобы отменить назначение пользователя в качестве владельца устройства на клиентском устройстве:

1. Выполните следующую команду в командной строке на клиентском устройстве:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -remove_owner
   ```

2. Введите имя пользователя и пароль.

Если пользователь входит во внутреннюю группу безопасности, учетная запись должна содержать имя пользователя.

Если пользователь входит в группу безопасности Active Directory, учетная запись должна содержать имя пользователя и имя домена.

Необходимо ввести временный одноразовый пароль (TOTP) из приложения для двухфакторной аутентификации.

Назначение пользователя владельцем устройства отменено.

Включение защиты учетной записи от несанкционированного изменения

Вы можете дополнительно включить защиту учетной записи пользователя от несанкционированного изменения. Если этот параметр включен, изменение параметров учетной записи пользователя требует авторизации пользователя с правами на изменение.

Чтобы включить или выключить защиту учетной записи от несанкционированного изменения:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Нажмите на учетную запись внутреннего пользователя, для которой вы хотите настроить защиту учетной записи от несанкционированного изменения.
3. В открывшемся окне свойств пользователя выберите вкладку **Двухфакторная аутентификация**.
4. На вкладке **Двухфакторная аутентификация** выберите **Запрашивать аутентификацию для проверки разрешения на изменение учетных записей пользователей**, если требуется запрашивать учетные данные и одноразовый код безопасности для двухфакторной аутентификации при каждом изменении параметров учетной записи. Или выберите **Разрешить пользователям изменять эту учетную запись без дополнительной аутентификации**.
5. Сохраните изменения.

Настройка двухфакторной аутентификации

Двухфакторная аутентификация включена автоматически, начиная с Сервера администрирования версии 16.1. Глобальный параметр выключения двухфакторной аутентификации не поддерживается. Этот сценарий содержит шаги по настройке двухфакторной аутентификации при первом входе в систему и настройке параметров двухфакторной аутентификации на Сервере администрирования.

Этапы

Настройка двухфакторной аутентификации 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).

   Доступно в России:

   - Kaspersky Password Manager для бизнеса (рекомендуется)
   - Bitrix24 OTP

- Yandex ID
- Avanpost Authenticator
- Aladdin 2FA
- Рутокен OTP

Доступно во всем мире (включая Россию):

- Google Authenticator
- Microsoft Authenticator

Чтобы проверить, поддерживает ли Kaspersky Security Center Linux приложение для аутентификации, которое вы хотите использовать, включите двухфакторную аутентификацию для всех пользователей или для определенного пользователя.

Один из шагов предполагает, что вы указываете код безопасности, сгенерированный приложением для аутентификации. Если проверка проходит успешно, значит Kaspersky Security Center Linux поддерживает выбранное приложение для аутентификации.

> Категорически не рекомендуется устанавливать приложение для аутентификации на то же устройство, с которого управляется Сервер администрирования.

2. **Синхронизация времени на устройстве с приложением аутентификации со временем 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. Для большей точности рекомендуется использовать одни и те же NTP-серверы во всей вашей инфраструктуре. Иначе возможны сбои при настройке двухфакторной аутентификации.

3. **Настройка двухфакторной аутентификации для учетных записей пользователей при входе в Web Console**

   Выполните вход в Web Console и настройте двухфакторную аутентификацию.

   Если вам недоступна настройка двухфакторной аутентификации, обратитесь к пользователю, у которого есть право Изменение списков управления доступом объектов в функциональной области **Общие функции: Права пользователей** и для которого настроена двухфакторная аутентификация, чтобы добавить вашу учетную запись в список допущенных к настройке двухфакторной аутентификации.

4. **Настройка параметров двухфакторной аутентификации на Сервере администрирования**

   Если вы настроили двухфакторную аутентификацию и у вас есть право Изменение списков управления доступом объектов в функциональной области **Общие функции**: **Права пользователей**, вы можете настроить следующие параметры двухфакторной аутентификации на Сервере администрирования:

   1. Просмотр списка пользователей, которые могут настроить двухфакторную аутентификацию при входе в систему:

      - Для чистой установки Сервера администрирования 16.1: добавьте нужных пользователей в список разрешений для настройки двухфакторной аутентификации, чтобы они могли настроить двухфакторную аутентификацию при первом входе в систему.
      - Для обновления или восстановления Сервера администрирования до версии 16.1: просмотрите список пользователей с правом настраивать двухфакторную аутентификацию и удалите учетные записи, которые не должны иметь доступа к Серверу администрирования.

2. Исключение учетных записей пользователей, для которых не требуется включать двухфакторную аутентификацию (не обязательно).

   Исключите учетные записи пользователей из двухфакторной аутентификации, чтобы разрешить им войти на Сервер администрирования, даже если у них не настроена двухэтапная проверка. Исключение учетных записей из двухэтапной проверки может потребоваться для учетных записей, которые не могут предоставить код безопасности во время аутентификации. Интеграционные учетные записи используются для запуска скриптов с помощью OpenAPI.

3. Сброс или удаление секретного ключа двухфакторной аутентификации (не обязательно).

   Вы можете сбросить секретный ключ двухфакторной аутентификации, если пользователь теряет доступ к своему устройству двухфакторной аутентификации или ему нужно настроить двухфакторную аутентификацию на новом устройстве. Вы также можете сбросить секретный ключ для своей учетной записи.

   Вы можете удалить секретный ключ, чтобы полностью заблокировать вход пользователя в Web Console и запретить пользователю доступ к Серверу администрирования.

4. Изменение имени издателя кода безопасности (не обязательно)

   Если у вас несколько Серверов администрирования с похожими именами, возможно, вам придется изменить имена издателей кода безопасности для лучшего распознавания разных Серверов администрирования.

Результаты

После выполнения этого сценария:

- Двухфакторная аутентификация настраивается как для вашей учетной записи, так и для другой учетной записи пользователя, которому требуется доступ к Серверу администрирования.
- Интеграционные учетные записи исключены из двухфакторной аутентификации.

О двухфакторной аутентификации учетной записи

Kaspersky Security Center Linux предоставляет двухфакторную аутентификацию для пользователей Kaspersky Security Center Web Console. Двухфакторная аутентификация основана на стандарте RFC 6238 (TOTP: Time-Based One-Time Password algorithm – алгоритм временных одноразовых паролей).

При каждом входе в Kaspersky Security Center Web Console пользователь вводит свое имя пользователя, пароль и дополнительный одноразовый код безопасности. Для получения одноразовых кодов безопасности необходимо установить на компьютере или мобильном устройстве приложение для аутентификации.

Может использоваться любое приложение для аутентификации, поддерживающее алгоритм временных одноразовых паролей (TOTP), например, Google Authenticator. Для генерации одноразового кода безопасности системное время, установленное на устройстве с приложением для аутентификации, должно быть синхронизировано со временем, установленным на устройстве с Сервером администрирования. Для большей точности рекомендуется использовать одни и те же NTP-серверы во всей вашей инфраструктуре.

Чтобы проверить, поддерживает ли Kaspersky Security Center Linux то или иное приложение для аутентификации, достаточно попытаться пройти двухфакторную аутентификацию с помощью этого приложения.

На одном из шагов процедуры вводится код безопасности, сгенерированный приложением для аутентификации. Если проверка проходит успешно, значит Kaspersky Security Center Linux поддерживает выбранное приложение для аутентификации.

Генерация секретного кода с помощью приложения 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.

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. После следующего входа в систему Серверу администрирования будет присвоено новое имя издателя кода безопасности. Код безопасности является одноразовым и действует до 30 секунд (точное время может варьироваться).

Настоятельно рекомендуется сохранить секретный ключ (или QR-код) и хранить его в надежном месте. Этот поможет вам восстановить доступ к Kaspersky Security Center Web Console в случае потери доступа к мобильному устройству.

Следует учитывать следующие особенности двухфакторной аутентификации:

- Начиная с версии 16.1, двухфакторная аутентификация на Сервере администрирования включается автоматически, а возможность настройки двухфакторной аутентификации при входе в систему выключена по умолчанию. Настройка двухфакторной аутентификации при входе доступна только пользователям, включенным в список разрешений для настройки двухфакторной аутентификации.
- Пользователь может настроить двухфакторную аутентификацию только для своей учетной записи.
- Пользователь может исключить учетные записи из двухфакторной аутентификации. Это может быть необходимо для интеграционных учетных записей, для которых невозможно получение одноразового кода безопасности для аутентификации. Интеграционные учетные записи используются для запуска скриптов с помощью OpenAPI.
- Для генерации нового секретного ключа двухфакторной аутентификации пользователь должен сбросить секретный ключ для своей учетной записи.
- Для сброса или удаления секретного ключа двухфакторной аутентификации других пользователей необходима учетная запись с настроенной двухфакторной аутентификацией и правом Изменение списков управления доступом объектов в функциональной области **Общие функции**: **Права пользователей**.
- Для исключения учетных записей пользователей из двухфакторной аутентификации или изменения списка разрешений для настройки аутентификации необходима учетная запись с настроенной двухфакторной аутентификацией и с правом Изменение списков управления доступом объектов в функциональной области **Общие функции**: **Права пользователей**.

- Всегда должен быть хотя бы один пользователь с настроенной двухфакторной аутентификацией, чтобы этот пользователь мог управлять списком пользователей с правом настраивать двухфакторную аутентификацию и списком исключений.

- Двухфакторная аутентификация автоматически включается только для Серверов администрирования версии 16.1. Параметры двухфакторной аутентификации главных или подчиненных Серверов администрирования версии 16 или более ранних останутся неизменными.

- Виртуальные Серверы администрирования наследуют параметры двухфакторной аутентификации от соответствующего физического Сервера администрирования, поэтому, если на физическом Сервере администрирования двухфакторная аутентификация включена, она также включается и на виртуальном Сервере администрирования. Настройка параметров двухфакторной аутентификации на виртуальном Сервере администрирования не поддерживается.

- Для правильной работы двухфакторной аутентификации необходимо обновить Сервер администрирования и Web Console до версии 16.1 или более поздней.

Для обеспечения комплексной защиты с помощью двухфакторной аутентификации должна быть обеспечена безопасность не только Сервера администрирования, но и устройства, на котором Сервер установлен. Соответствующие рекомендации приведены в Руководстве по усилению защиты.

Настройка секретного ключа двухфакторной аутентификации при входе в Kaspersky Security Center Web Console

При первом входе в Kaspersky Security Center Linux 16.1 или выше откроется окно для настройки двухфакторной аутентификации.

Чтобы настроить двухфакторную аутентификацию для учетной записи:

1. Установите любое приложение, поддерживающее алгоритм временных одноразовых паролей (TOTP), на мобильном устройстве или компьютере.

   Доступно в России:

   - Kaspersky Password Manager для бизнеса (рекомендуется)
   - Bitrix24 OTP
   - Yandex ID
   - Avanpost Authenticator
   - Aladdin 2FA
   - Рутокен OTP

   Доступно во всем мире (включая Россию):

   - Google Authenticator
   - Microsoft Authenticator

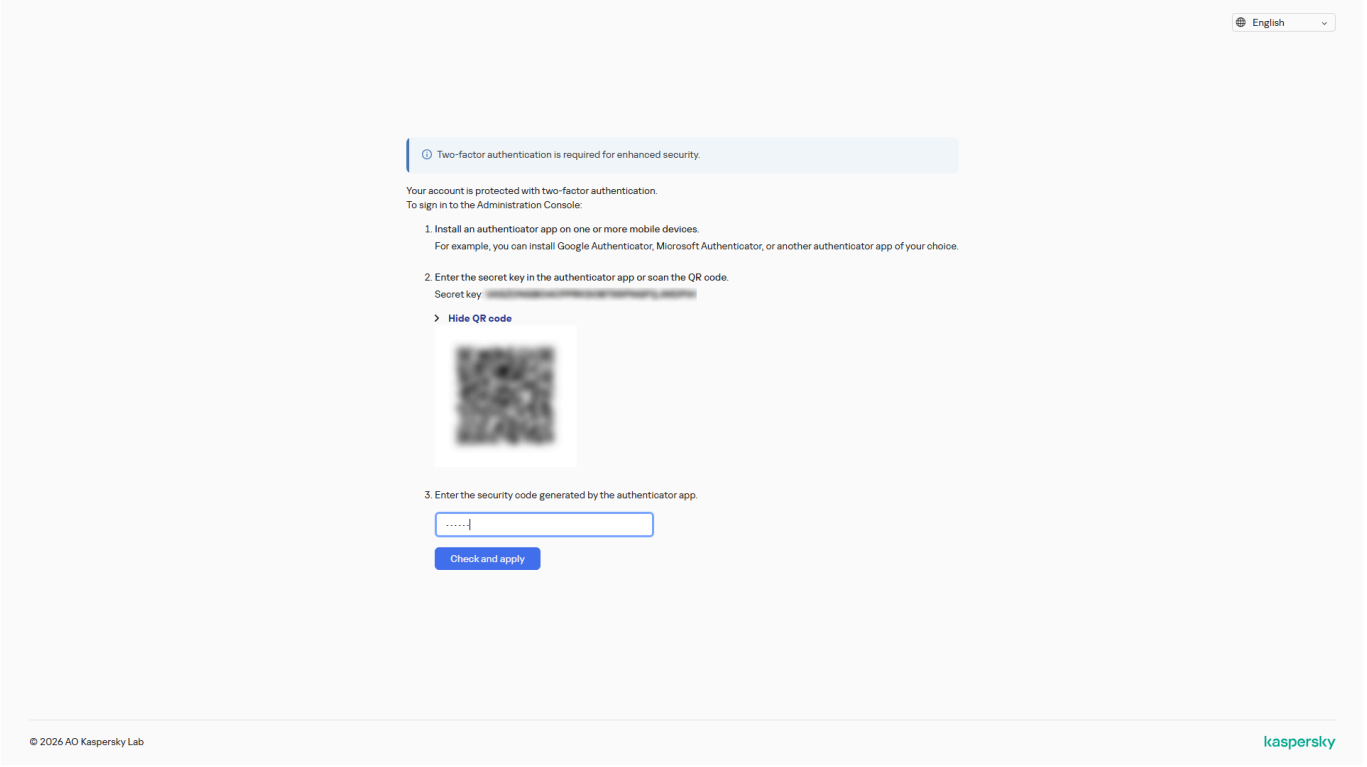
Категорически не рекомендуется устанавливать приложение для аутентификации на то же устройство, с которого управляется Сервер администрирования.

2. Убедитесь, что время на устройстве с приложением для аутентификации и время на устройстве с Сервером администрирования синхронизированы с UTC. Для большей точности рекомендуется использовать одни и те же NTP-серверы во всей вашей инфраструктуре.

3. Сгенерируйте одноразовый код безопасности с помощью приложения для аутентификации на мобильном устройстве или компьютере. Для этого выполните одно из следующих действий:

   - Вручную введите секретный ключ двухфакторной аутентификации в приложение для аутентификации.
   - Нажмите на кнопку **Просмотреть QR-код** и отсканируйте QR-код с помощью приложения для аутентификации.

   На мобильном устройстве отобразится одноразовый код безопасности из 6 цифр.



Настройка секретного ключа двухфакторной аутентификации при входе в Kaspersky Security Center Web Console

4. В окне **Двухфакторная аутентификация** укажите код безопасности, сгенерированный приложением для аутентификации, и нажмите на кнопку **Проверить и применить**.

   Конфигурация Рутокена OTP

   Если вы используете Рутокен OTP, вам потребуется мобильное устройство Android с установленным приложением Рутокен OTP. Мобильное устройство Android должно соответствовать следующим требованиям:

   - Операционная система Android 7 или выше.
   - NFC-модуль доступен и включен.

В приложении Рутокен OTP необходимо настроить следующие параметры:

- Выполните проверку QR-кода, который отображается в двухэтапном мастере настройки.
- Установите временной интервал – 30 секунд.
- Выберите алгоритм SHA1.

Чтобы настроить Рутокен OTP:

1. Поместите устройство Рутокена OTP рядом с мобильным устройством с NFC-модулем.
2. В приложении Рутокен OTP нажмите **Подключить токен**.
3. В приложении Рутокен OTP нажмите **Настроить параметры**, а затем нажмите **Сохранить секретный ключ**.

   Если токен успешно подключен к мобильному устройству, приложение Рутокен OTP отображает следующие сообщения:

   - **Токен подключен.**
   - **Параметры настроены.**
   - **Секретный ключ сохранен.**
4. На устройстве Рутокен OTP нажмите на кнопку.

   На устройстве отобразится код безопасности.
5. В Kaspersky Security Center Web Console в окне двухфакторной аутентификации введите код безопасности.

Двухфакторная аутентификация для вашей учетной записи настроена. У вас есть доступ к Серверу администрирования в соответствии со своими правами.

Если вам недоступна настройка двухфакторной аутентификации, обратитесь к пользователю, у которого есть право Изменение списков управления доступом объектов в функциональной области **Общие функции**: **Права пользователей** и который настроил двухфакторную аутентификацию, чтобы добавить вашу учетную запись в список пользователей с правом настраивать двухфакторную аутентификацию.

Разрешение для настройки двухфакторной аутентификации пользователям

Список разрешений для настройки двухфакторной аутентификации – это список пользователей, которым разрешена начальная настройка двухфакторной аутентификации при входе в Web Console. В этот список входят учетные записи пользователей, для которых не настроена двухфакторная аутентификация. По умолчанию новые учетные записи не включаются в список разрешений для настройки двухфакторной аутентификации и должны добавляться в этот список администратором. Если новая учетная запись является интеграционной и используется для запуска скриптов OpenAPI, ее необходимо исключить из двухфакторной аутентификации.

Учетная запись пользователя автоматически удаляется из списка, когда для нее настраивается двухфакторная аутентификация или она добавляется в исключения из двухфакторной аутентификации.

Вручную изменять список разрешений для настройки двухфакторной аутентификации разрешено учетным записям с настроенной двухфакторной аутентификацией и правом Изменение списков управления доступом объектов в функциональной области **Общие функции**: **Права пользователей**.

Чтобы добавить учетную запись пользователя из списка разрешений для настройки двухфакторной аутентификации вручную:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Двухфакторная аутентификация** в окне свойств в таблице **Пользователям разрешено генерировать секретные ключи** нажмите на кнопку **Добавить**.

3. В открывшемся окне:

   a. Выберите учетную запись пользователя, которую вы хотите добавить.

      В список пользователей с правом настраивать двухфакторную аутентификацию могут добавляться только пользователи, которые не исключены из двухфакторной аутентификации и не имеют секретного ключа двухфакторной аутентификации.

   b. Если учетная запись защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите ваши собственные учетные данные и одноразовый код безопасности для двухфакторной аутентификации.

   c. Сохраните изменения.

Выбранная учетная запись пользователя будет добавлена в список разрешений для настройки двухфакторной аутентификации. При следующем входе в систему этому пользователю будет предоставлена возможность сгенерировать секретный ключ.

Удаление учетной записи пользователя из списка разрешений для настройки двухфакторной аутентификации возможно до тех пор, пока для этой учетной записи не будет настроена двухфакторная аутентификация.

Чтобы удалить учетные записи пользователей из списка разрешений для настройки двухфакторной аутентификации вручную:

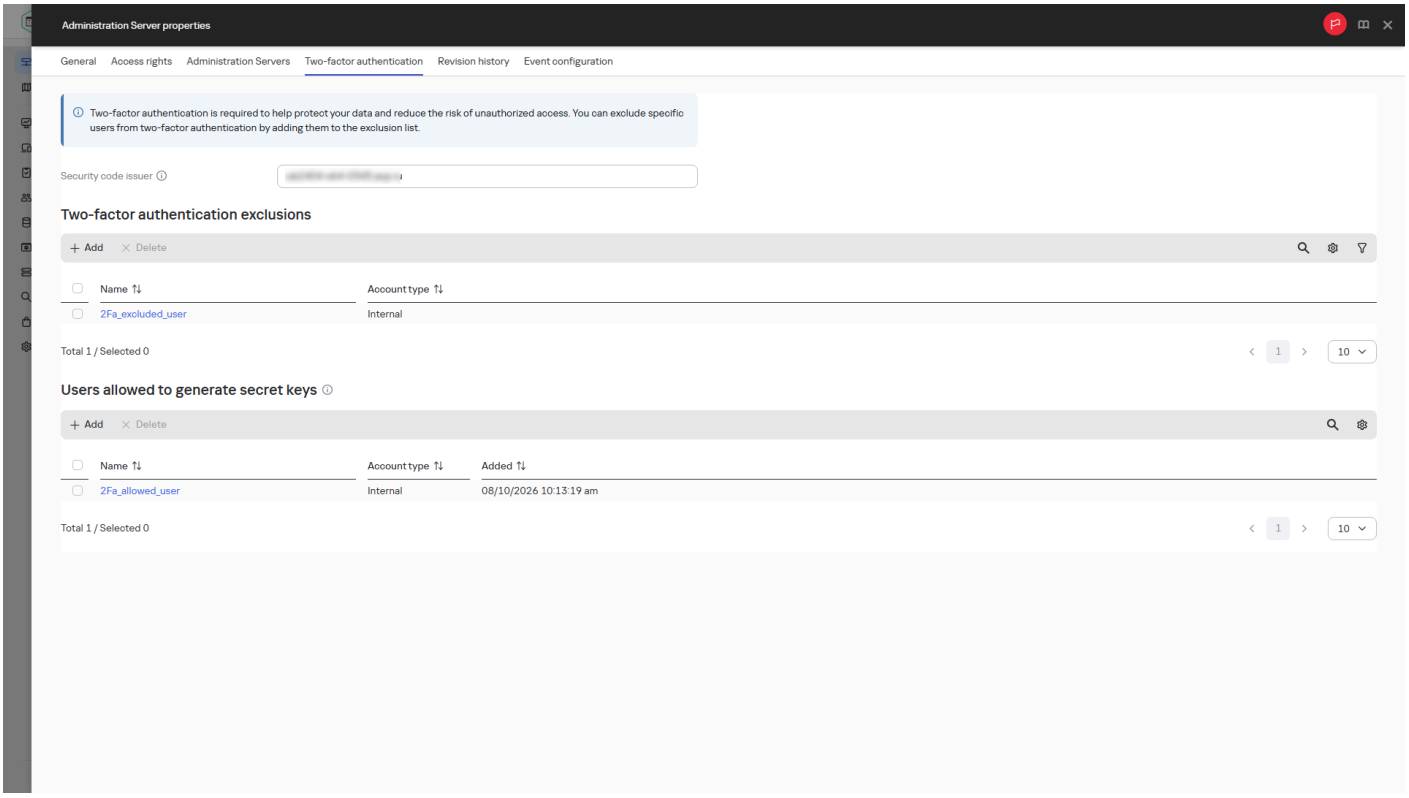
1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Двухфакторная аутентификация** в окне свойств, в таблице **Пользователям разрешено генерировать секретные ключи**, выберите учетные записи, которые требуется удалить, и нажмите на кнопку **Удалить**.

3. Если учетная запись защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите ваши собственные учетные данные и одноразовый код безопасности для двухфакторной аутентификации.

Выбранные учетные записи пользователей будут удалены из списка разрешений для настройки двухфакторной аутентификации.



Настройка списка разрешений для настройки двухфакторной аутентификации

Если во время активного сеанса на Сервере администрирования ваш секретный ключ двухфакторной аутентификации удален другим пользователем или вы сбросили ключ самостоятельно, не создав нового, возможность вносить изменения в список пользователей с правом настраивать двухфакторную аутентификацию будет заблокирована.

Учетные записи пользователей также могут добавляться в список разрешений для настройки двухфакторной аутентификации и удаляться из него автоматически.

При сбросе секретного ключа двухфакторной аутентификации для других учетных записей такие учетные записи автоматически добавляются в список пользователей с правом настраивать двухфакторную аутентификацию, чтобы пользователь мог сгенерировать для себя новый секретный ключ.

При обновлении Сервера администрирования с версии 16 или ниже до версии 16.1 или выше, а также при создании резервной копии данных на Сервере администрирования версии 16 или ниже и восстановлении из нее на Сервере администрирования версии 16.1 или выше учетные записи пользователей добавляются в список пользователей с правом настраивать двухфакторную аутентификацию автоматически, если выполняются следующие условия:

- У пользователя есть право на чтение в функциональной области *Общие функции: Базовая функциональность*, назначенное непосредственно пользователю (не через группу безопасности). Область применения роли пользователя с этим разрешением должна включать все управляемые и нераспределенные устройства и должна быть задана на уровне Сервера администрирования.
- Пользователь не входит в список исключений из двухфакторной аутентификации.
- У пользователя отсутствует секретный ключ двухфакторной аутентификации.
- На Сервере администрирования предыдущей версии двухфакторная аутентификация не была включена для всех пользователей.

Невыполнение хотя бы одного из условий приведет к тому, что пользователь не будет добавлен в список пользователей с правом настраивать двухфакторную аутентификацию.

После обновления или восстановления из резервной копии рекомендуется убедиться, что список пользователей с правом настраивать двухфакторную аутентификацию содержит только те учетные записи пользователей, у которых должен быть доступ к Серверу администрирования. Просмотрите список разрешений для настройки двухфакторной аутентификации и удалите из него все лишние учетные записи. Добавьте интегрированные учетные записи, используемые для запуска скриптов через OpenAPI, в список исключений – это необходимо для правильной работы скриптов.

Учетные записи пользователей потеряют доступ к Серверу администрирования после обновления или восстановления, если будут выполнены все следующие условия:

- У пользователя есть право на чтение в функциональной области *Общие функции: Базовая функциональность*, назначенное через группу безопасности (а не непосредственно пользователю), либо вовсе нет этого права.
- Пользователь не входит в список исключений из двухфакторной аутентификации.
- У пользователя отсутствует секретный ключ двухфакторной аутентификации.
- На Сервере администрирования предыдущей версии двухфакторная аутентификация была включена для всех пользователей.

При необходимости эти учетные записи можно добавить вручную в список разрешений для настройки двухфакторной аутентификации.

Сброс и удаление секретного ключа двухфакторной аутентификации

Сброс секретного ключа может потребоваться, если пользователь утратит доступ к своему устройству двухфакторной аутентификации или возникнет необходимость настроить двухфакторную аутентификацию на новом устройстве. Сброс секретного ключа позволяет пользователю войти в Web Console и сгенерировать новый секретный ключ.

Вы можете сбросить или удалить секретный ключ двухфакторной аутентификации для учетных записей других пользователей, только если у вас настроена двухфакторная аутентификация и есть право Изменение списков управления доступом объектов в функциональной области **Общие функции**: **Права пользователей**. Вы также можете сгенерировать новый секретный ключ для себя.

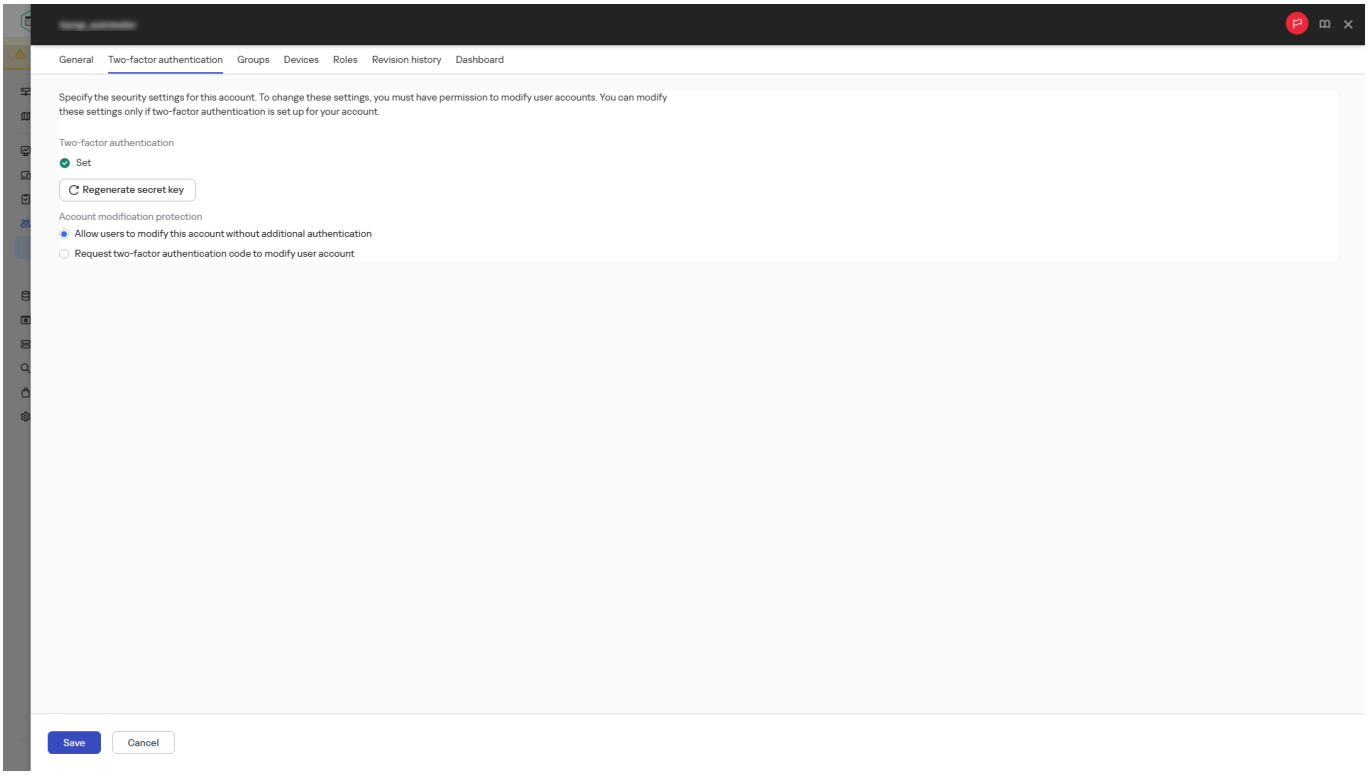
Чтобы сбросить секретный ключ для учетной записи:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.

2. Нажмите на имя учетной записи, для которой нужно сбросить секретный ключ.

3. Если необходимо сбросить секретный ключ для собственной учетной записи:

   a. На вкладке **Двухфакторная аутентификация** нажмите на кнопку **Сгенерировать секретный ключ снова**.

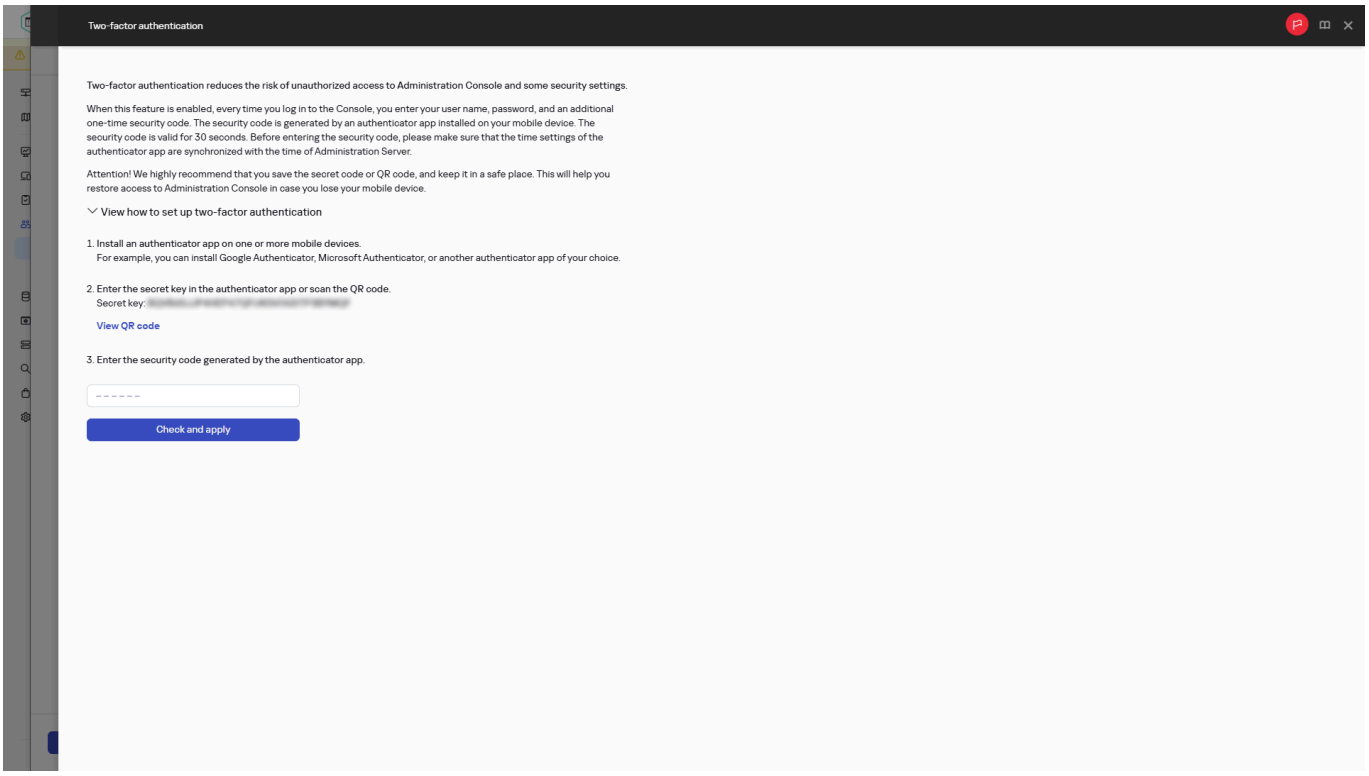


Восстановление секретного ключа двухфакторной аутентификации для текущей учетной записи пользователя

   a. Если ваша учетная запись защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите ваши собственные учетные данные и код двухфакторной аутентификации.

   b. В окне **Двухфакторная аутентификация** нажмите **Узнайте, как настроить двухфакторную аутентификацию**, затем **Просмотреть QR-код**.

   c. Отсканируйте QR-код в приложении для аутентификации на мобильном устройстве, чтобы получить одноразовый код безопасности.



Настройка нового секретного ключа двухфакторной аутентификации для текущей учетной записи пользователя

a. В окне **Двухфакторная аутентификация** укажите одноразовый код безопасности, сгенерированный приложением для аутентификации, нажмите на кнопку **Проверить и применить**, затем сохраните изменения.

Конфигурация Рутокена OTP

Если вы используете Рутокен OTP, вам потребуется мобильное устройство Android с установленным приложением Рутокен OTP. Мобильное устройство Android должно соответствовать следующим требованиям:

- Операционная система Android 7 или выше.
- NFC-модуль доступен и включен.

В приложении Рутокен OTP необходимо настроить следующие параметры:

- Выполните проверку QR-кода, который отображается в двухэтапном мастере настройки.
- Установите временной интервал – 30 секунд.
- Выберите алгоритм SHA1.

Чтобы настроить Рутокен OTP:

1. Поместите устройство Рутокена OTP рядом с мобильным устройством с NFC-модулем.
2. В приложении Рутокен OTP нажмите **Подключить токен**.
3. В приложении Рутокен OTP нажмите **Настроить параметры**, а затем нажмите **Сохранить секретный ключ**.

Если токен успешно подключен к мобильному устройству, приложение Рутокен OTP отображает следующие сообщения:

- **Токен подключен.**
- **Параметры настроены.**
- **Секретный ключ сохранен.**

4. На устройстве Рутокен OTP нажмите на кнопку.

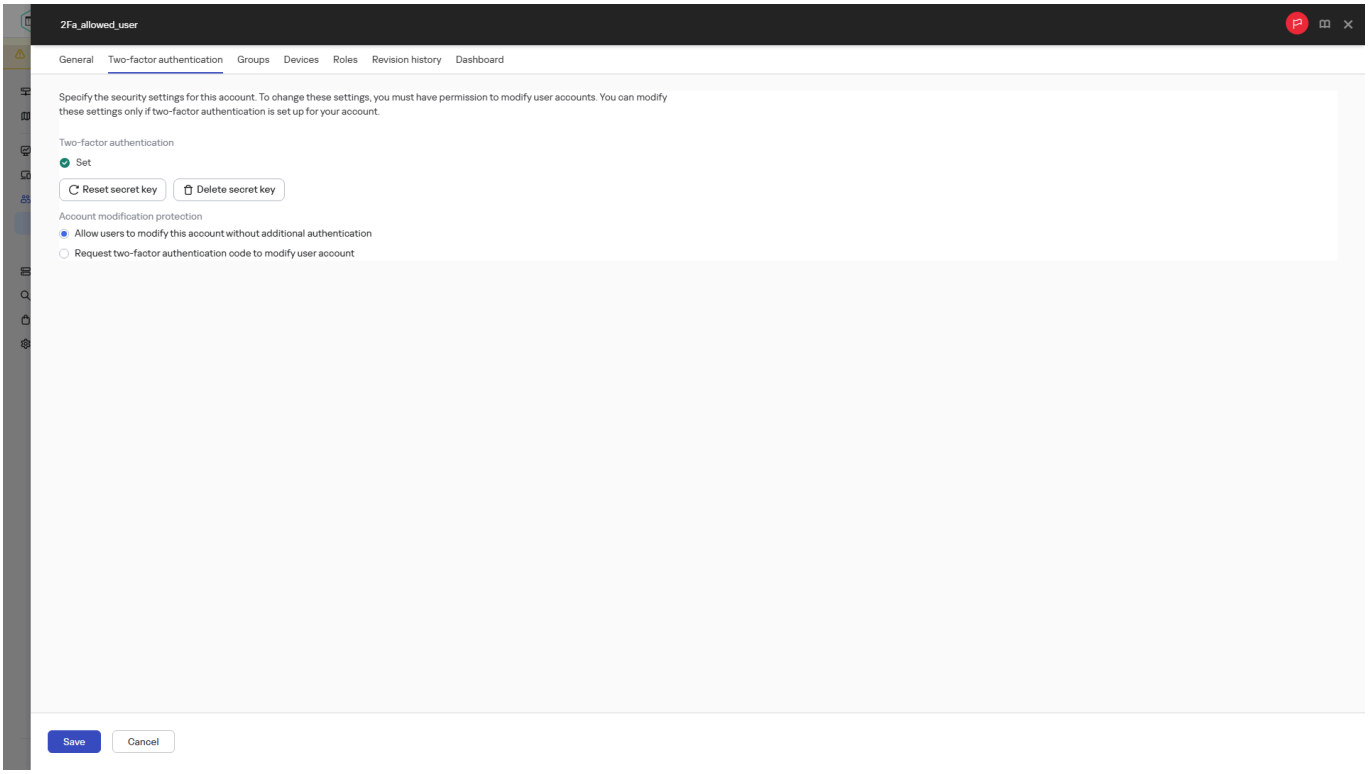
   На устройстве отобразится код безопасности.

5. В Kaspersky Security Center Web Console в окне двухфакторной аутентификации введите код безопасности.

Секретный ключ вашей собственной учетной записи изменен.

4. Если необходимо сбросить секретный ключ для чужой учетной записи:

   a. На вкладке **Двухфакторная аутентификация** нажмите на кнопку **Сбросить секретный ключ**.



Сброс секретного ключа двухфакторной аутентификации для другой учетной записи пользователя

   a. Если учетная запись защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите ваши собственные учетные данные и одноразовый код безопасности для двухфакторной аутентификации.

   b. Подтвердите сброс секретного ключа, а затем сохраните изменения.

При сбросе секретного ключа для другой учетной записи существующий секретный ключ удаляется, а учетная запись добавляется в список разрешений для настройки двухфакторной аутентификации в свойствах Сервера администрирования. При следующем входе в систему пользователь сможет сгенерировать новый секретный ключ.

Секретный ключ учетной записи пользователя будет сброшен.

Вы можете удалить секретный ключ, чтобы полностью заблокировать вход пользователя в Web Console и запретить пользователю доступ к Серверу администрирования.

Чтобы удалить секретный ключ:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Нажмите на имя внутренней учетной записи, для которой требуется удалить секретный ключ.

   Секретный ключ для собственной учетной записи удалить невозможно.

3. На вкладке **Двухфакторная аутентификация** нажмите на кнопку **Удалить секретный ключ**.
4. Если учетная запись защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите ваши собственные учетные данные и одноразовый код безопасности для двухфакторной аутентификации.
5. Подтвердите удаление секретного ключа, а затем сохраните изменения.

Секретный ключ учетной записи пользователя будет удален.

Для восстановления доступа пользователя можно добавить в список разрешений для настройки двухфакторной аутентификации в свойствах Сервера администрирования. В этом случае при следующем входе в систему пользователь сможет сгенерировать новый секретный ключ.

Исключение учетных записей из двухфакторной аутентификации

Учетные записи пользователей можно исключить из двухфакторной аутентификации, чтобы разрешить им входить на Сервер администрирования, даже если у них не настроена двухфакторная аутентификация. Исключение учетных записей из двухфакторной аутентификации может потребоваться для интегрированных учетных записей, которые по техническим причинам не могут предоставлять одноразовый код безопасности во время аутентификации. Интегрированные учетные записи используются для запуска скриптов с помощью OpenAPI.

Вносить изменения в список исключений могут учетные записи с настроенной двухфакторной аутентификацией и правом Изменение списков управления доступом объектов в функциональной области **Общие функции**: **Права пользователей**.

Чтобы исключить учетную запись пользователя из двухфакторной аутентификации:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Двухфакторная аутентификация** окна свойств в таблице **Исключения двухфакторной аутентификации** нажмите на кнопку **Добавить**.

3. В открывшемся окне:

   a. Выберите учетную запись пользователя, которую вы хотите исключить.

   b. Если учетная запись защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите ваши собственные учетные данные и одноразовый код безопасности для двухфакторной аутентификации.

   c. Сохраните изменения.

Выбранные учетные записи пользователей будут исключены из двухфакторной аутентификации, а их секретные ключи (если таковые существуют) будут удалены. Список исключенных учетных записей не изменяется при восстановлении из резервной копии на Сервере администрирования версии 16.1 или при обновлении Сервера администрирования до версии 16.1 или более поздней. Если в предыдущей версии Сервера администрирования у учетных записей из списка исключений были секретные ключи, в версии 16.1 эти секретные ключи будут удалены.

Удаление учетных записей пользователей из списка исключений полностью запрещает таким пользователям вход в Web Console и не позволяет им осуществлять доступ к Серверу администрирования.

Чтобы удалить учетные записи пользователей из списка исключений:

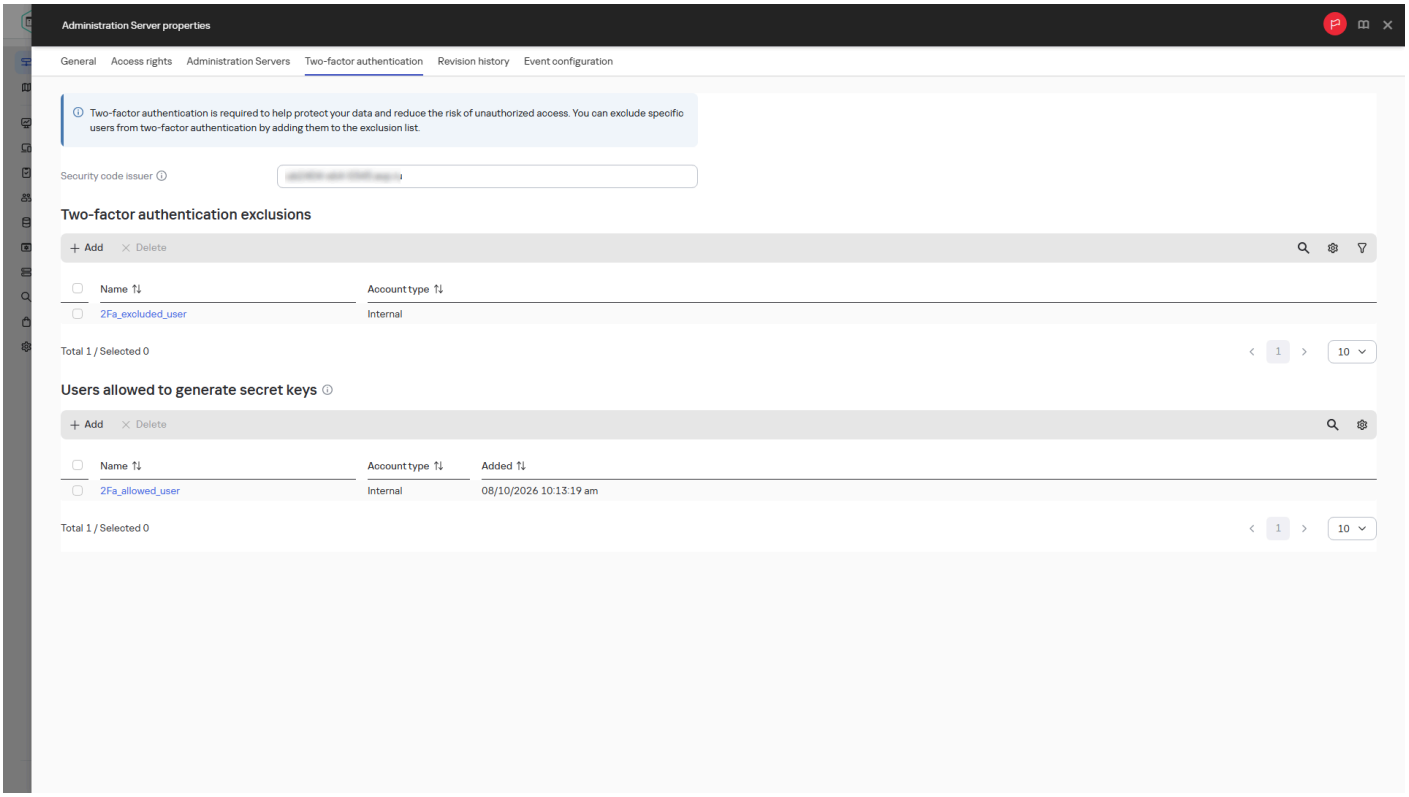
1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. В окне свойств, на вкладке **Двухфакторная аутентификация**, в таблице **Исключения двухфакторной аутентификации**, выберите учетные записи, которые требуется удалить, и нажмите на кнопку **Удалить**.

3. Если учетная запись защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите ваши собственные учетные данные и одноразовый код безопасности для двухфакторной аутентификации.

Выбранные учетные записи пользователей будут удалены из списка исключений.



Настройка списка исключений двухфакторной аутентификации

Изменение имени издателя кода безопасности

У вас может быть несколько идентификаторов (далее также издателями) для разных Серверов администрирования. Вы можете изменить имя издателя кода безопасности, например, Сервер администрирования уже использует аналогичное имя издателя кода безопасности для другого Сервера администрирования. По умолчанию имя издателя кода безопасности совпадает с именем Сервера администрирования.

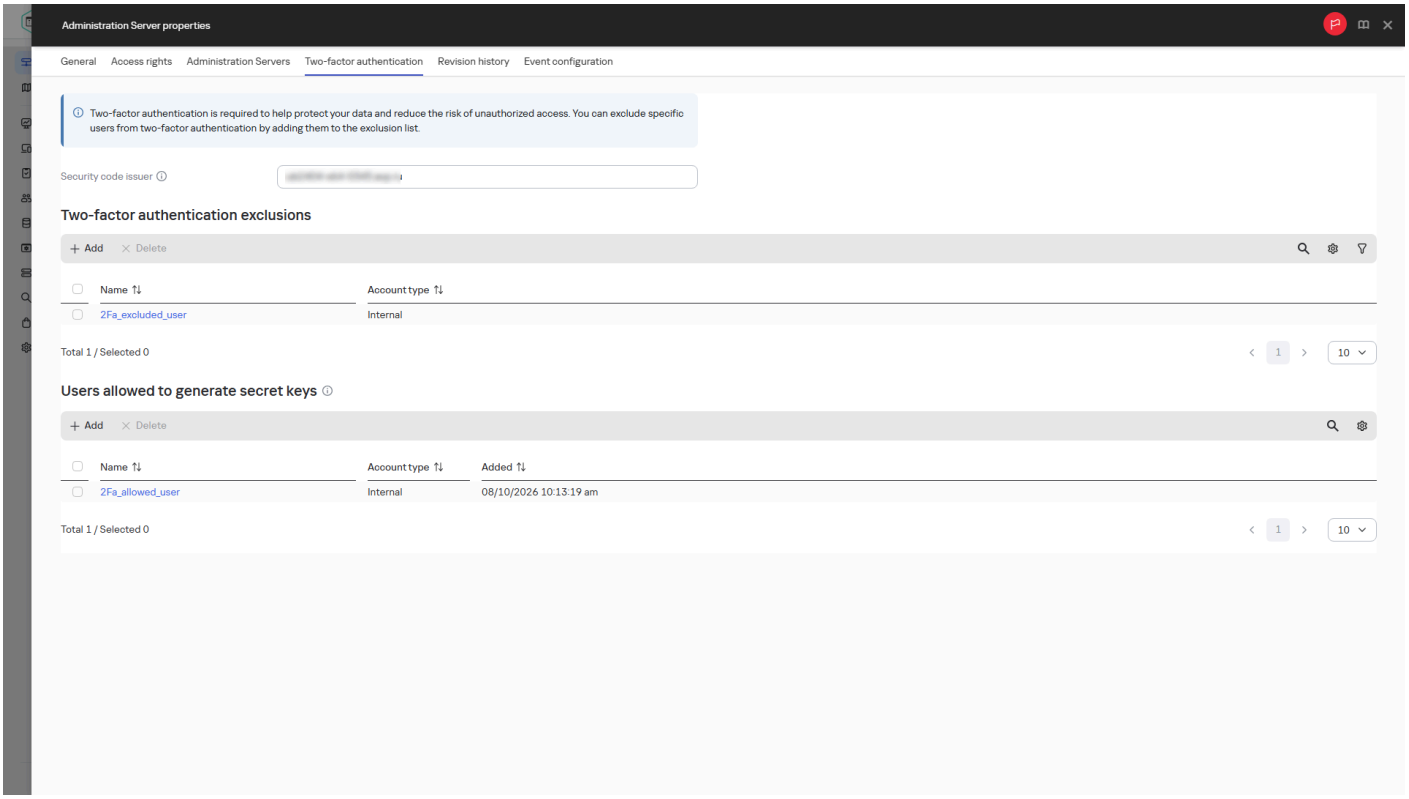
Чтобы указать новое имя издателя кода безопасности:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Двухфакторная аутентификация** в окне свойств введите новое имя в поле **Кем выдан код безопасности**, а затем сохраните изменения.

После следующего входа в систему Серверу администрирования будет присвоено новое имя издателя кода безопасности.



Ввод имени 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:

1. На устройстве, на котором установлен Сервер администрирования, запустите командную строку Linux.

2. Для утилиты klscflag выполните следующую команду:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
   ```

где N – количество попыток ввода пароля.

3. Чтобы изменения вступили в силу, перезапустите службу Сервера администрирования.

Максимальное количество попыток ввода пароля изменено.

Удаление пользователей или групп безопасности

Можно удалять только внутренних пользователей или группы безопасности.

Удаление пользователей или групп безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи** или **Группы**.

2. Установите флажок рядом с именем пользователя или группы безопасности, которую требуется удалить.

   Всегда должен быть хотя бы один пользователь с настроенной двухфакторной аутентификацией, чтобы этот пользователь мог управлять списком пользователей с правом настраивать двухфакторную аутентификацию и списком исключений.

3. Нажмите на кнопку **Удалить**.

4. В появившемся окне нажмите на кнопку **ОК**.

Пользователь или группа безопасности удалены.

Изменение пароля учетной записи пользователя

Вам может потребоваться изменить пароль своей учетной записи или учетной записи другого пользователя, если срок действия текущего пароля истекает или если вы хотите сменить его на более надежный.

Пароль должен соответствовать следующим правилам:

- Длина пароля должна быть от 8 до 256 символов.
- Пароль должен содержать символы как минимум трех групп из 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 "@", если "." расположена перед "@".

Изменение пароля своей учетной записи

Чтобы изменить пароль вашей учетной записи:

1. В верхней панели откройте меню своей учетной записи, нажав на ее имя.
2. В раскрывающемся списке выберите **Изменение пароля**.
3. В открывшейся правой панели введите текущий пароль и укажите новый пароль для подключения к Kaspersky Security Center Linux.

   Чтобы посмотреть введенный пароль, нажмите на кнопку .
4. Если ваша учетная запись защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите учетные данные вашей учетной записи или учетной записи, у которой есть право Изменение списков управления доступом объектов в функциональной области **Общие функции**: **Права пользователей**.
5. Введите одноразовый код безопасности, сгенерированный в приложении для аутентификации на мобильном устройстве.

Изменение пароля учетной записи внутреннего пользователя

Чтобы изменить пароль учетной записи внутреннего пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Выберите учетную запись пользователя, которую требуется изменить.
3. В открывшемся окне свойств пользователя на вкладке **Общие** нажмите на кнопку **Изменение пароля**.
4. Установите новый пароль для подключения пользователя к Kaspersky Security Center Linux.

   Чтобы посмотреть введенный пароль, нажмите на кнопку .
5. При необходимости включите параметр **Пользователю нужно сменить пароль при первом входе**, чтобы принудительно изменить пароль при следующей аутентификации пользователя.

6. Если учетная запись пользователя защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите учетные данные учетной записи, у которой есть право Изменение списков управления доступом объектов в функциональной области **Общие функции**: **Права пользователей**.

7. Введите одноразовый код безопасности, сгенерированный в приложении для аутентификации на мобильном устройстве.

Настройка параметров изменения пароля с помощью флагов сервера

Запустите командную строку 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`. Запустите следующие команды:

- Настройка периода замены пароля (флаг `LP_SplPwdChangePeriodDays`).

  `./klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <период_ротации>`

  где `<период_ротации>` – это период в днях, по истечении которого срок действия пароля пользователя истекает. Возможные значения: 0–730. Если значение параметра указано 0, смена пароля выключена.

- Настройка времени предварительного предупреждения о необходимости изменения пароля (флаг `LP_SplPwdChangeNotificationHours`).

  `./klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <время_предупреждения>`

  где `<время_предупреждения>` – это период в часах, перед тем как срок действия пароля пользователя истечет. В течение этого времени отображается уведомление о необходимости изменить пароль. Возможные значения: 0–17520. Если значение параметра указано 0, время предупреждения составляет 25% от периода замены пароля.

- Указание значения по умолчанию для параметра **Пользователю нужно сменить пароль при первом входе** (флаг `LP_SplPwdForceChange`).

  `./klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <значение>`

  Где возможные значения флага `<значение>`:

  `1` – параметр **Пользователю нужно сменить пароль при первом входе** включен.

  `0` – параметр **Пользователю нужно сменить пароль при первом входе** выключен.

Чтобы просмотреть текущее значение флага, выполните следующую команду:

`./klscflag -fget -pv .core/.independent -s KLLIM -n <флаг> -t d`

Где `<флаг>` – это флаг `LP_SplPwdChangePeriodDays`, `LP_SplPwdChangeNotificationHours` или `LP_SplPwdForceChange`.

Создание роли пользователя

Чтобы создать роль пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Имя новой роли** укажите имя новой роли.
4. Нажмите на кнопку **ОК**, чтобы применить изменения.
5. В открывшемся окне измените параметры роли:
   - На вкладке **Общие** измените имя роли.

     Вы не можете изменять имена предопределенных ролей.
   - На вкладке **Параметры** измените область действия роли, а также политики и профили политик, связанные с ролью.
   - На вкладке **Права доступа** измените права доступа к приложениям "Лаборатории Касперского".
6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Созданная роль появится в списке ролей пользователей.

Изменение роли пользователя

Чтобы изменить роль пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Выберите роль, которую требуется изменить.
3. В открывшемся окне измените параметры роли:
   - На вкладке **Общие** измените имя роли.

     Вы не можете изменять имена предопределенных ролей.
   - На вкладке **Параметры** измените область действия роли, а также политики и профили политик, связанные с ролью.
   - На вкладке **Права доступа** измените права доступа к приложениям "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 приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи** или **Группы**.

2. Установите флажки напротив имен пользователей или групп безопасности, которые требуется добавить в область роли.

3. Нажмите на кнопку **Назначить роль**.

   Будет запущен мастер назначения роли. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. На шаге **Выбор роли** выберите роль, которую требуется назначить.

5. На шаге **Определение области** выберите группу администрирования, которую требуется добавить в область роли.

6. Нажмите на кнопку **Назначить роль**, чтобы закрыть окно мастера.

Выбранные пользователи, группы безопасности и группы администрирования добавлены в область роли.

Способ 2:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.

2. Выберите роль, для которой требуется задать область.

3. В открывшемся окне свойств роли выберите вкладку **Параметры**.

4. В разделе **Область действия роли** нажмите на кнопку **Добавить**.

   Будет запущен мастер назначения роли. Для продолжения работы мастера нажмите на кнопку **Далее**.

5. На шаге **Определение области** выберите группу администрирования, которую требуется добавить в область роли.

6. На шаге **Выбор пользователей** выберите пользователей и группы безопасности, которые требуется добавить в область роли.

7. Нажмите на кнопку **Назначить роль**, чтобы закрыть окно мастера.

8. Нажмите на кнопку **Закрыть** (⨯), чтобы закрыть окно свойств.

Выбранные пользователи, группы безопасности и группы администрирования добавлены в область роли.

Способ 3:

1. В главном окне приложения нажмите на имя 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, примените и сохраните изменения.

   Выбранные пользователи или группы безопасности добавлены в область роли.

Удаление роли пользователя

Чтобы удалить роль пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.

2. Установите флажок напротив роли, которую требуется удалить.

3. Нажмите на кнопку **Удалить**.

4. В появившемся окне нажмите на кнопку **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 приложений городской навигации для всех устройств группы администрирования. Приложения городской навигации необходимы для работы только одного устройства пользователя, выполняющего роль курьера, в группе администрирования "Пользователи". В этом случае можно назначить роль "Курьер" владельцу этого устройства и создать профиль политики, разрешающий использовать приложения городской навигации на устройствах, владельцам которых назначена роль "Курьер". Все остальные параметры политики остаются без изменений. Только пользователям с ролью "Курьер" разрешено использовать приложения городской навигации. Затем, если другому сотруднику будет назначена роль "Курьер", этот сотрудник также сможет использовать приложения городской навигации на устройстве, принадлежащем вашей организации. Однако использование приложений городской навигации будет запрещено на других устройствах этой группы администрирования.

Чтобы связать роль с профилем политики:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Выберите роль, которую требуется связать с профилем политики.

   Откроется окно свойств роли на вкладке **Общие**.
3. Перейдите на вкладку **Параметры** и прокрутите вниз до раздела **Политики**.
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 приложения 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 окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Перейдите в раздел **Иерархия Серверов администрирования**.

3. Включите параметр **Передать список ролей подчиненному Серверу администрирования** и нажмите на кнопку **Сохранить**.

Приложение 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.

Смена пароля учетной записи

Вы можете изменить пароль локальной учетной записи, например, когда пользователь забыл пароль локальной учетной записи или чтобы изменить пароль по расписанию.

Изменение пароля будет применяться, даже если пользователь не вошел в учетную запись. Вы также можете изменить пароль для локальной учетной записи root.

Эту задачу можно выполнять только на устройствах под управлением Linux.

Чтобы изменить пароль локальной учетной записи на определенных устройствах:

1. В главном окне приложения перейдите в раздел **Задачи**.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. В поле **Тип задачи** выберите **Изменить пароль учетной записи (только для Linux)**.

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 определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

   Назначить задачу выборке устройств

   Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

   Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

   Задача *Изменить пароль учетной записи (только для Linux)* создается для указанных устройств. Если вы выбрали параметр **Назначить задачу группе администрирования**, задача является групповой.

5. На шаге **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

   Доступные параметры зависят от параметра, выбранного на предыдущем шаге.

6. На шаге **Введите имя учетной записи и новый пароль** укажите следующие параметры:

   - В поле **Имя учетной записи** укажите имя учетной записи, для которой вы хотите изменить пароль.

   - В поле **Новый пароль** укажите пароль, который будет установлен для учетной записи, указанной в предыдущем поле.

     Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

   - При необходимости установите флажок **Установить в качестве одноразового пароля (пользователь должен изменить пароль после первого входа в систему)**.

     Установить в качестве одноразового пароля (пользователь должен изменить пароль после первого входа в систему)

     Если этот флажок установлен, пользователю будет предложено изменить новый пароль после первого входа в систему.

     Если этот флажок снят, пользователю не будет предлагаться изменить новый пароль после первого входа в систему.

     По умолчанию флажок снят.

7. На шаге **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

   Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи. В этом окне можно проверить параметры задачи, изменить их или при необходимости настроить расписание запуска задачи.

8. В списке задач выберите созданную задачу и нажмите на кнопку **Запустить**.

   Или дождитесь запуска задачи в соответствии с расписанием, указанным в параметрах задачи.

Когда задача изменения пароля учетной записи завершится, пароль будет изменен для указанной локальной учетной записи на выбранных устройствах.

Чтобы обеспечить корректную работу задач изменения пароля учетной записи, на пользовательском устройстве должен быть выключен SELinux.

Отзыв прав локального администратора

Вы можете отозвать права локального администратора для учетных записей. Это дает вам дополнительный уровень контроля учетных записей пользователей. Например, вы можете отозвать права локального администратора после завершения разового назначения.

При запуске этой задачи указанная локальная учетная запись проверяется на принадлежность к локальным группам администраторов, которые определены в параметрах политики Агента администрирования. Вы можете настроить список локальных групп администраторов в параметрах политики Агента администрирования. Вы также можете проверить список учетных записей привилегированных пользователей, используя **Отчет о привилегированных пользователях устройств (только для Linux)**.

Эту задачу можно выполнять только на устройствах под управлением Linux.

Чтобы отозвать права локального администратора на определенных устройствах:

1. В главном окне приложения перейдите в раздел **Задачи**.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. В поле **Тип задачи** выберите **Отозвать права локального администратора (только для Linux)**.

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 определенное приложение 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.

Для указанных устройств создается задача *Отозвать права локального администратора (только для Linux)*. Если вы выбрали параметр **Назначить задачу группе администрирования**, задача является групповой.

5. На шаге **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

   Доступные параметры зависят от параметра, выбранного на предыдущем шаге.

6. На этом шаге мастера укажите следующие параметры:

   - В группе параметров **Режим работы** выберите режим работы:

     Отозвать права локального администратора для перечисленных учетных записей

     Если выбран этот параметр, права локального администратора будут отозваны для указанных локальных учетных записей.

     По умолчанию выбран этот вариант.

     Исключить перечисленные учетные записи из списка отзыва прав локального администратора

     Если выбран этот параметр, права локального администратора будут отозваны для всех локальных учетных записей, кроме указанных.

     По умолчанию вариант не выбран.

   - Укажите локальные учетные записи:

     - Нажмите на кнопку **Добавить**.
     - В открывшемся окне выполните одно из следующих действий:
       - В поле **Имя учетной записи** укажите имя локальной учетной записи.
       - В группе параметров **Действие учетной записи** (доступно, если выбран параметр **Отозвать права локального администратора для перечисленных учетных записей**) выберите действие.
       - **Сохранить учетную запись**

         Если выбран этот параметр, локальная учетная запись не удаляется после отзыва прав локального администратора.

         По умолчанию выбран этот вариант.

       - **Удалить учетную запись**

Если выбран этот параметр, локальная учетная запись будет удалена независимо от того, есть ли у нее права локального администратора.

По умолчанию вариант не выбран.

7. На шаге **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

   Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи. В этом окне можно проверить параметры задачи, изменить их или при необходимости настроить расписание запуска задачи.

8. В списке задач выберите созданную задачу и нажмите на кнопку **Запустить**.

   Или дождитесь запуска задачи в соответствии с расписанием, указанным в параметрах задачи.

После завершения задачи права локального администратора отозваны для указанных локальных учетных записей на выбранных устройствах.

Настройка доменной аутентификации Kerberos

Kaspersky Security Center Linux позволяет использовать доменную аутентификацию по протоколу Kerberos. Доменная аутентификация позволяет вам включить безопасную аутентификацию в Kaspersky Security Center Web Console без повторного ввода пароля в корпоративной сети (единый вход).

Сначала вам нужно настроить контроллер домена для использования Kerberos и создать файл keytab. Подробнее см. документацию к контроллеру домена.

SCRIL (для интерактивного входа требуется смарт-карта) поддерживается для Microsoft Active Directory.

Создание файла keytab для FreeIPA и AldPro

Чтобы создать файл keytab:

1. Создайте учетную запись, которая будет использоваться IAM для доступа к контроллеру домена.

2. Если Сервер администрирования находится за пределами домена FreeIPA/AldPro, добавьте запись DNS и запись устройства:

   ```
   ipa dnsrecord-add <zoneName> <recordName> --a-rec <IP-адрес Сервера администрирования>
   ipa host-add --password=<password> <адрес устройства Сервера администрирования>
   ```

3. Укажите тип PAC при создании HTTP-сервиса для Сервера администрирования:

   ```
   ipa service-add HTTP/<FQDN устройства Сервера администрирования>@<ДОМЕН, НАПИСАННЫЙ ЗАГЛАВНЫМИ БУКВАМИ> --ok-to-auth-as-delegate=true --pac-type PAD
   ```

4. Укажите учетную запись для аутентификации:

   ```
   ipa service-allow-retrieve-keytab HTTP/<адрес устройства Сервера администрирования>@<ДОМЕН, НАПИСАННЫЙ ЗАГЛАВНЫМИ БУКВАМИ> --user=<user>
   ```

5. Экспортируйте файл keytab:

```
ipa-getkeytab -s <адрес контроллера домена> -p HTTP/<адрес устройства Сервера администрирования>@<ДОМЕН, НАПИСАННЫЙ ЗАГЛАВНЫМИ БУКВАМИ> -k /tmp/h.keytab
```

Создание файла keytab для Microsoft Active Directory

Чтобы создать файл keytab:

1. Создайте учетную запись, которая будет использоваться IAM для связи с контроллером домена.

2. Включите следующие параметры для учетной записи:

   - **Запрет изменения пароля пользователем.**
   - **Kerberos AES 256-разрядное шифрование.**

   Вы можете включить параметр **Срок действия пароля не ограничен**, чтобы избежать повторной выдачи файла keytab каждый раз, когда истекает срок действия пароля.

3. Добавьте имя субъекта-службы (SPN) в учетную запись:

```
setspn -S HTTP/<FQDN устройства Сервера администрирования> <ДОМЕН, НАПИСАННЫЙ ЗАГЛАВНЫМИ БУКВАМИ>\<user>
```

4. Экспортируйте файл keytab:

```
ktpass -out C:\<folder>\<имя файла keytab> -princ HTTP/<FQDN устройства Сервера администрирования>@<ДОМЕН, НАПИСАННЫЙ ЗАГЛАВНЫМИ БУКВАМИ> -mapuser <ДОМЕН, НАПИСАННЫЙ ЗАГЛАВНЫМИ БУКВАМИ>\<user> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass <password> -mapop set
```

Создание файла keytab для Samba

Чтобы создать файл keytab:

1. Создайте учетную запись, которая будет использоваться IAM для связи с контроллером домена:

```
samba-tool user add <user>
```

2. Добавьте имя субъекта-службы к учетной записи:

```
samba-tool spn add HTTP/<FQDN устройства Сервера администрирования> <user>
```

3. Экспортируйте файл keytab:

```
samba-tool domain exportkeytab /tmp/file.keytab --principal=HTTP/<FQDN устройства Сервера администрирования>
```

Включение доменной аутентификации Kerberos

Чтобы включить доменную аутентификацию Kerberos:

1. Выполните опрос контроллеров домена.
2. В главном окне приложения перейдите в раздел **Параметры** → **Единый вход**.
3. Включите параметр **Аутентификация Kerberos**.
4. Загрузите файл keytab.
5. Назначьте доменным пользователям роль, которая предоставляет доступ к Kaspersky Security Center Web Console.

   Доменная аутентификация Kerberos включена для доменных пользователей.

Обновление баз и приложений "Лаборатории Касперского"

В этом разделе описаны шаги, которые вам нужно выполнить для регулярных обновлений:

- баз и модулей приложений "Лаборатории Касперского";
- установленных приложений "Лаборатории Касперского", включая компоненты Kaspersky Security Center Linux и приложений безопасности.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"

В этом разделе представлен сценарий регулярного обновления баз данных, модулей приложений и приложений "Лаборатории Касперского". После того, как вы завершили сценарий Настройка защиты в сети организации, вам нужно поддерживать надежность системы защиты, чтобы обеспечить защиту Серверов администрирования и управляемых устройств от различных угроз, включая вирусы, сетевые атаки и фишинговые атаки.

Защита сети поддерживается обновленной с помощью регулярных обновлений следующего:

- баз и модулей приложений "Лаборатории Касперского";
- установленных приложений "Лаборатории Касперского", включая компоненты Kaspersky Security Center Linux и приложений 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 приложения безопасности.
- Антивирусные базы и другие базы данных "Лаборатории Касперского", критически важные для безопасности сети, всегда актуальны.

Предварительные требования

Управляемые устройства должны иметь соединение с Сервером администрирования. Если у устройств нет соединения, рассмотрите возможность обновления баз, модулей приложений и приложений "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 приложения безопасности "Лаборатории Касперского" на управляемых устройствах в соответствии со сценарием развертывания приложений "Лаборатории Касперского" с помощью Kaspersky Security Center 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 приложений "Лаборатории Касперского" состоит из следующих этапов:

1. **Выбор схемы обновления**

   Есть несколько схем, которые вы можете использовать для установки обновлений для приложений безопасности. Выберите схему или несколько схем, которые лучше всего соответствуют требованиям вашей сети.

2. **Создание задачи для загрузки обновлений в хранилище Сервера администрирования**

   Эта задача автоматически создается в мастере первоначальной настройки Kaspersky Security Center. Если вы не запускали мастер первоначальной настройки, создайте задачу сейчас.

   Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования, а также обновления баз и модулей приложений для Kaspersky Security Center Linux. 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 Linux 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 **Включено** 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 модулей приложений "Лаборатории Касперского". Файл различий описывает различия между двумя версиями файлов базы или модулями приложения. Поэтому файлы различий занимают меньше места, чем целые файлы. В результате уменьшается трафик между Сервером администрирования или точками распространения и управляемыми устройствами. Чтобы использовать эту функцию, включите параметр **Скачать файлы различий** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования* и/или *Загрузка обновлений в хранилища точек распространения*.

   Инструкция: Использование файлов различий для обновления баз и модулей приложений "Лаборатории Касперского"

6. **Настройка автоматической установки обновлений для приложений безопасности**

   Создайте задачу *Обновление* для управляемых приложений, чтобы обеспечить своевременное обновление модулей приложений и баз данных "Лаборатории Касперского", в том числе антивирусных баз. Чтобы обеспечить своевременное обновление, рекомендуется при настройке расписания задачи выбрать вариант **При загрузке обновлений в хранилище**.

   Если обновление требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства.

7. **Одобрение и отклонение обновлений управляемых приложений "Лаборатории Касперского"**

   По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус обновления на *Одобрено* или *Отклонено*. Одобренные обновления всегда устанавливаются. Если обновление управляемых приложений "Лаборатории Касперского" требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства. Обновления, которым вы установили статус *Отклонено*, не устанавливаются на управляемые устройства. Если ранее отклоненное обновление для управляемого приложения было установлено, Kaspersky Security Center Linux попытается удалить обновления со всех устройств.

   Одобрение и отклонение обновлений доступно только для Агента администрирования и управляемых приложений "Лаборатории Касперского", установленных на клиентских устройствах под управлением Windows и Linux. Бесшовное обновление Сервера администрирования, Kaspersky Security Center Web Console и веб-плагинов управления не поддерживается.

   Инструкция: Одобрение и отклонение обновлений программного обеспечения.

   Иногда после обновления Агента администрирования вам может потребоваться перезагрузить управляемые устройства. Если отображается уведомление о необходимости перезагрузки, нажмите на ссылку **Просмотреть устройства** в уведомлении, установите флажки рядом с устройствами, которые требуется перезагрузить, и нажмите на кнопку **Перезагрузить**, чтобы завершить обновление Агента администрирования.

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, модулей приложений и приложений "Лаборатории Касперского"

Чтобы убедиться, что защита ваших Серверов администрирования и управляемых устройств актуальна, вам нужно своевременно предоставлять обновления следующего:

- Баз и модулей приложений "Лаборатории Касперского".

  Kaspersky Security Center Linux проверяет доступность серверов "Лаборатории Касперского" перед загрузкой баз и модулей приложений "Лаборатории Касперского". Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы. Это необходимо для обновления антивирусных баз и поддержания уровня безопасности управляемых устройств.

- установленных приложений "Лаборатории Касперского", включая компоненты Kaspersky Security Center Linux и приложений безопасности.

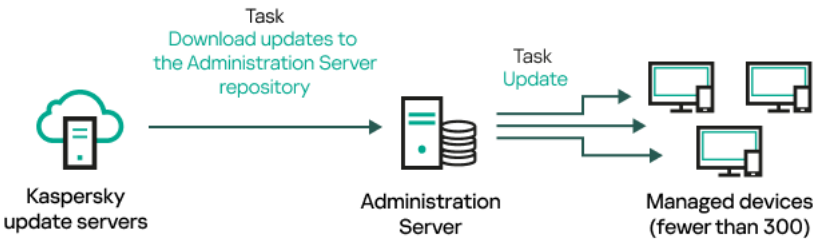
  Kaspersky Security Center Linux позволяет автоматически обновлять Агент администрирования и приложения "Лаборатории Касперского", установленные на клиентских устройствах под управлением Windows и Linux. Бесшовное обновление Сервера администрирования, Kaspersky Security Center Web Console и веб-плагинов управления не поддерживается. Для обновления этих компонентов вам необходимо скачать их последние версии с сайта "Лаборатории Касперского" и установить их вручную.

В зависимости от конфигурации вашей сети вы можете использовать следующие схемы загрузки и распространения необходимых обновлений на управляемые устройства:

- С помощью одной задачи: *Загрузка обновлений в хранилище Сервера администрирования*
- С помощью двух задач:
  - Задача *Загрузка обновлений в хранилище Сервера администрирования*.
  - Задача *Загрузка обновлений в хранилища точек распространения*.
- Вручную через локальную папку, общую папку или FTP-сервер
- Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security на управляемых устройствах
- Через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

Использование задачи Загрузка обновлений в хранилище Сервера администрирования

В этой схеме Kaspersky Security Center Linux 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).



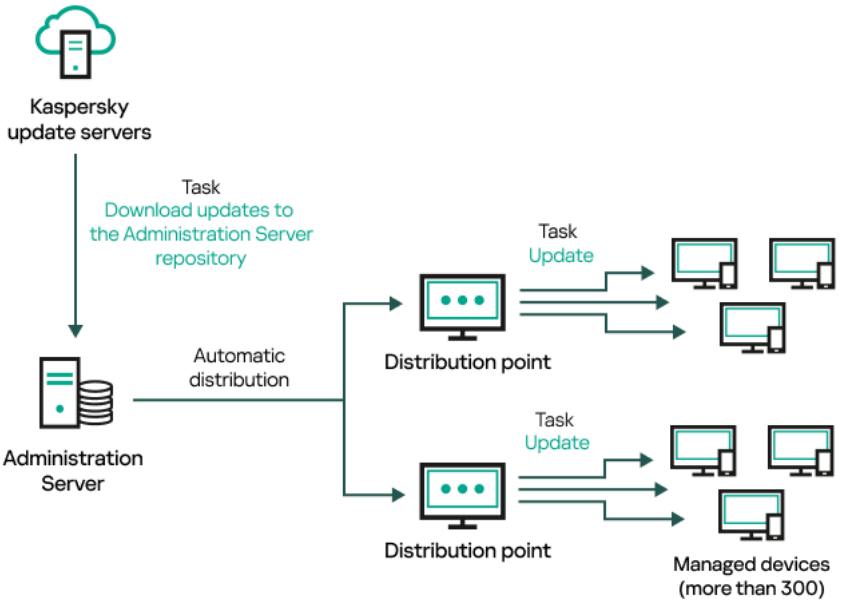
Обновление с использованием задачи *Загрузка обновлений в хранилище Сервера администрирования* и без точек распространения

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 модули приложений для Kaspersky Endpoint Security загружены в хранилище Сервера администрирования. Эти обновления устанавливаются с помощью задачи *Обновление* Kaspersky Endpoint Security.

Задача *Загрузка обновлений в хранилище Сервера администрирования* недоступна на виртуальных Серверах администрирования. В хранилище виртуального Сервера отображаются обновления, загруженные на главный Сервер администрирования.

Вы можете настроить проверку полученных обновлений на работоспособность и на наличие ошибок на наборе тестовых устройств. Если проверка прошла успешно, обновления распространяются на другие управляемые устройства.

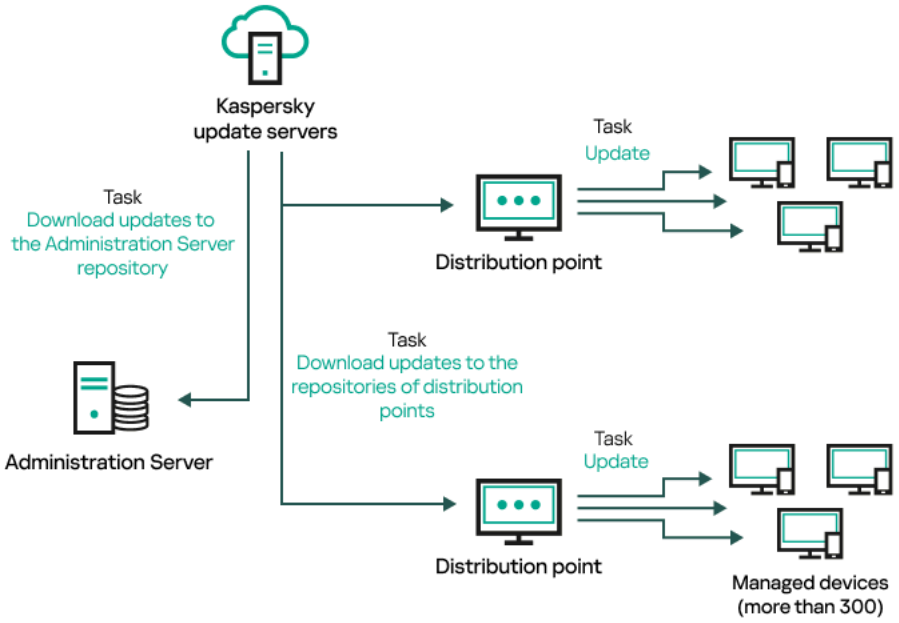
Каждое управляемое приложение "Лаборатории Касперского" запрашивает требуемые обновления с Сервера администрирования. Сервер администрирования объединяет эти запросы и загружает только те обновления, которые запрашиваются приложениями. Это обеспечивает то, что загружаются только нужные обновления и только один раз. При выполнении задачи *Загрузка обновлений в хранилище Сервера администрирования*, для обеспечения загрузки необходимых версий баз и модулей приложений "Лаборатории Касперского", на серверы обновлений "Лаборатории Касперского" автоматически, Сервер администрирования отправляет следующую информацию:

- идентификатор и версия приложения;
- идентификатор установки приложения;
- идентификатор активного ключа;
- идентификатор запуска задачи *Загрузка обновлений в хранилище Сервера администрирования*.

Передаваемая информация не содержит персональных данных и других конфиденциальных данных. АО "Лаборатория Касперского" защищает полученную информацию в соответствии с установленными законом требованиями.

Использование двух задач: Загрузка обновлений в хранилище Сервера администрирования и Загрузка обновлений в хранилища точек распространения

Вы можете загружать обновления в хранилища точек распространения непосредственно с серверов обновлений "Лаборатории Касперского" вместо хранилища Сервера администрирования, а затем распространять обновления на управляемые устройства (см. рисунок ниже). Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.



Обновление с использованием задачи *Загрузка обновлений в хранилище Сервера администрирования* и задачи *Загрузка обновлений в хранилища точек распространения*

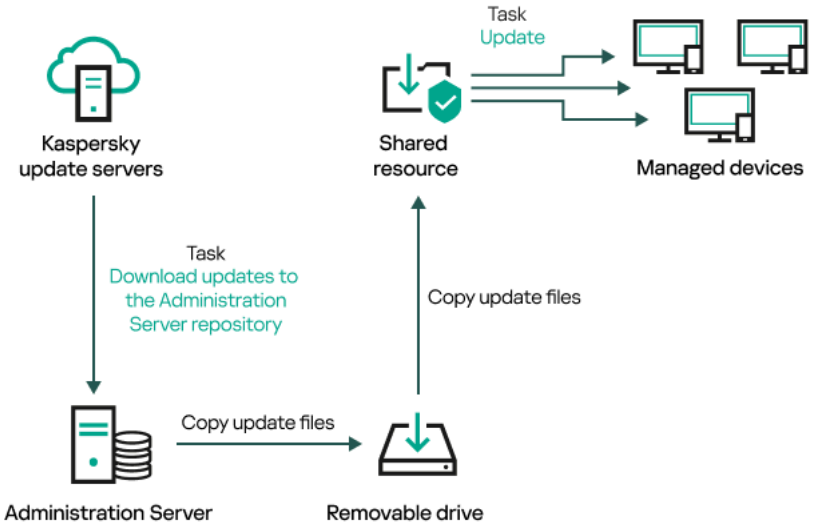
По умолчанию Сервер администрирования и точки распространения взаимодействуют с серверами обновлений "Лаборатории Касперского" и загружают обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования и/или точки распространения на использование протокола HTTP вместо HTTPS.

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 модулей приложений "Лаборатории Касперского" для Kaspersky Security Center Linux.

Вручную через локальную папку, общую папку или FTP-сервер

Если клиентские устройства не подключены к Серверу администрирования, вы можете использовать локальную папку или общий ресурс в качестве источника обновления баз, модулей приложений и приложений "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 (см. рисунок ниже).



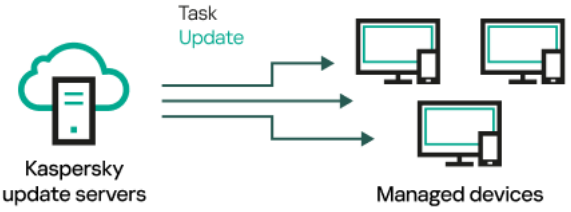
Обновление через локальную папку, общую папку или FTP-сервер

Подробнее об источниках обновлений в Kaspersky Endpoint Security см. в следующих справках:

- Справка Kaspersky Endpoint Security для Linux
- Справка Kaspersky Endpoint Security для Windows

Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security на управляемых устройствах

На управляемых устройствах вы можете настроить Kaspersky Endpoint Security на получение обновлений напрямую с серверов обновлений "Лаборатории Касперского" (см. рисунок ниже).



Обновление приложений безопасности непосредственно с серверов обновлений "Лаборатории Касперского"

В этой схеме приложение безопасности не использует хранилище, предоставленное Kaspersky Security Center Linux. Чтобы получать обновления непосредственно с серверов обновлений "Лаборатории Касперского", укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений в приложении безопасности. Дополнительные сведения об этих параметрах см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Linux
- Справка Kaspersky Endpoint Security для Windows

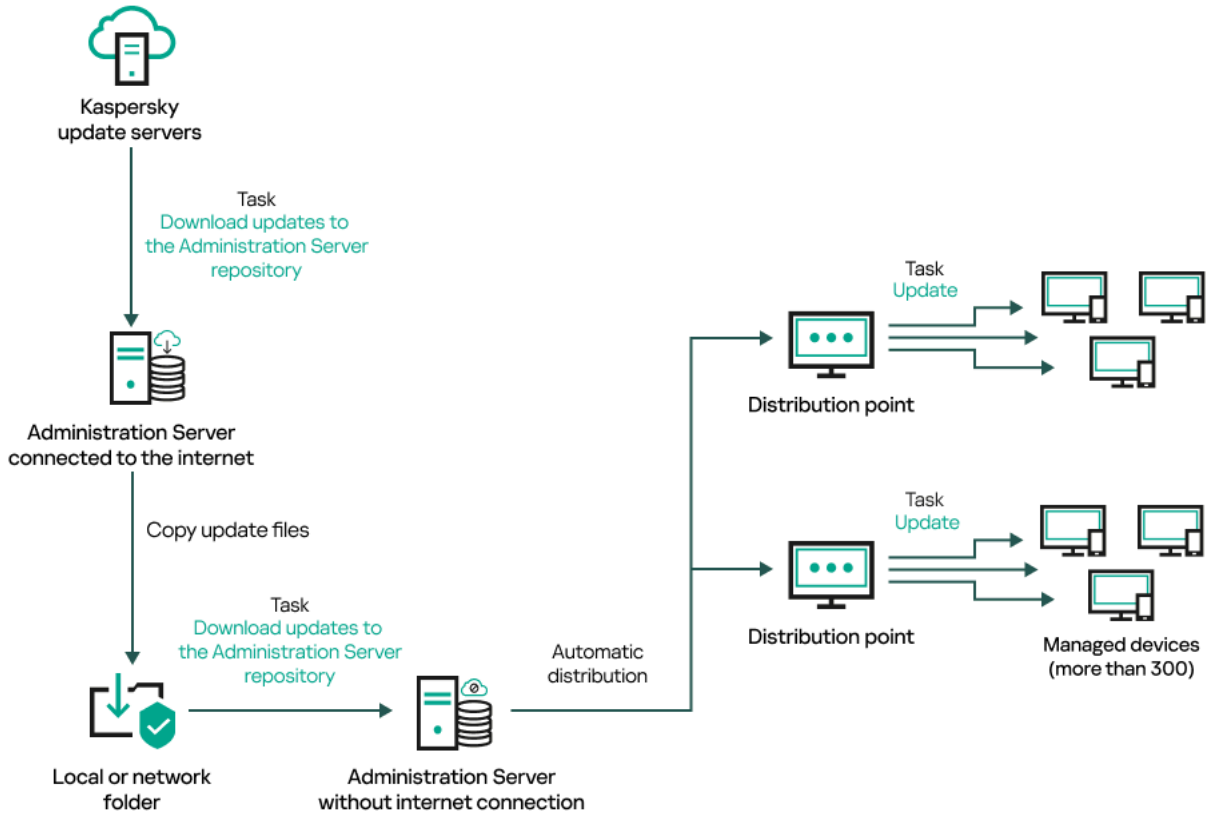
Через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

Если Сервер администрирования не имеет подключения к интернету, вы можете настроить задачу *Загрузка обновлений в хранилище Сервера администрирования* для загрузки обновлений из локальной или сетевой папки. В этом случае требуется время от времени копировать необходимые файлы обновлений в указанную папку. Например, вы можете скопировать необходимые файлы обновления из одного из следующих источников:

- Сервер администрирования, имеющий выход в интернет (см. рис. ниже).

  Так как Сервер администрирования загружает только те обновления, которые запрашиваются приложениями безопасности, наборы приложений безопасности, которыми управляют Серверы администрирования (подключенные и не подключенные к интернету) должны совпадать.

  Если Сервер администрирования, который вы используете для загрузки обновлений, имеет версию 13.2 или более раннюю, откройте свойства задачи *Загрузка обновлений в хранилище Сервера администрирования*, а затем включите параметр **Скачивать 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 *Скачивать обновления, используя старую схему*. Вы также можете настроить параметр *Загрузить файл запроса на обновление автоматически*, чтобы утилита Kaspersky Update Utility скачивала только необходимые обновления.

Создание задачи Загрузка обновлений в хранилище Сервера администрирования

Задача *Загрузка обновлений в хранилище Сервера администрирования* позволяет загружать обновления баз и модулей приложения безопасности "Лаборатории Касперского" с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования.

Задача *Загрузка обновлений в хранилище Сервера администрирования* создается автоматически при запуске 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.

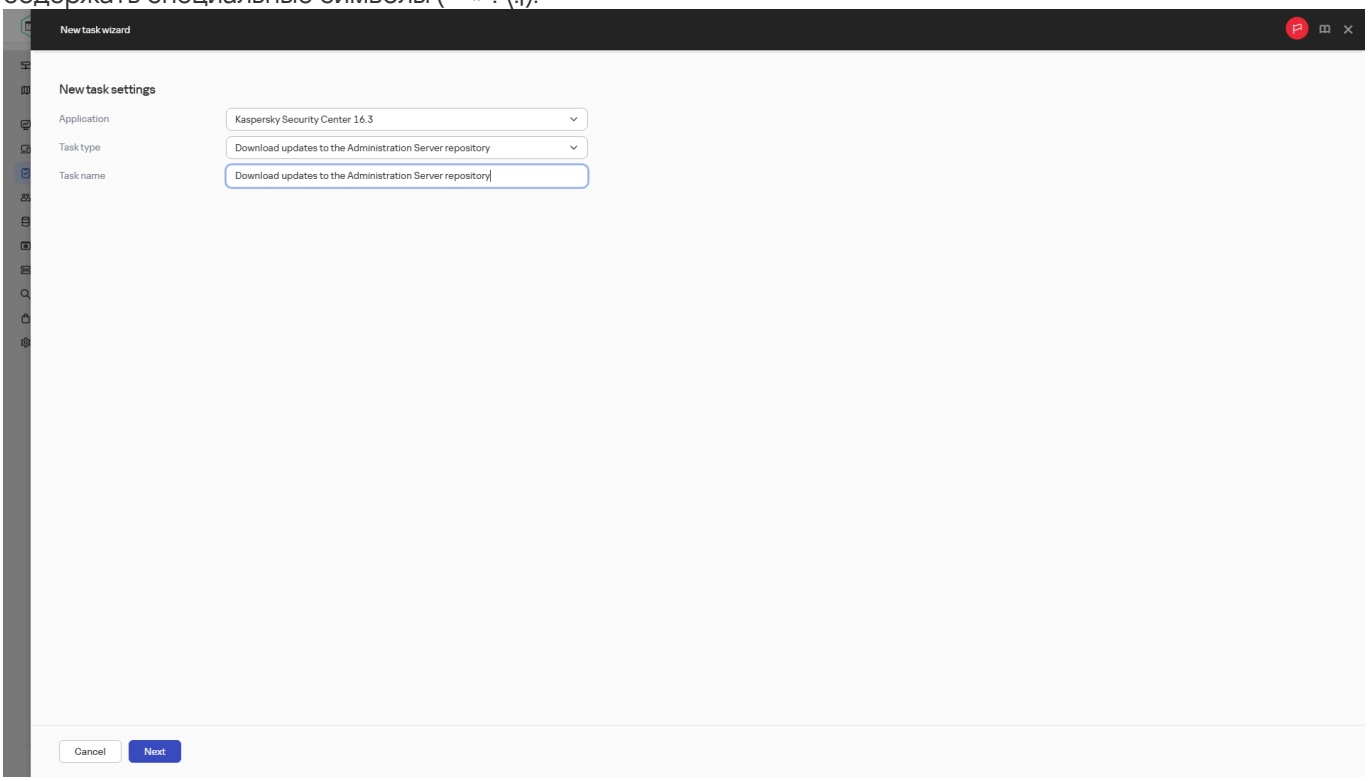
Перед распространением обновлений на управляемые устройства вы можете выполнить задачу *Проверка обновлений*. Это позволяет убедиться, что Сервер администрирования правильно установит загруженные обновления и уровень безопасности не снизится из-за обновлений. Чтобы проверить обновления перед распространением, настройте параметр **Выполнить проверку обновлений** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования*.

Чтобы создать задачу Загрузка обновлений в хранилище Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

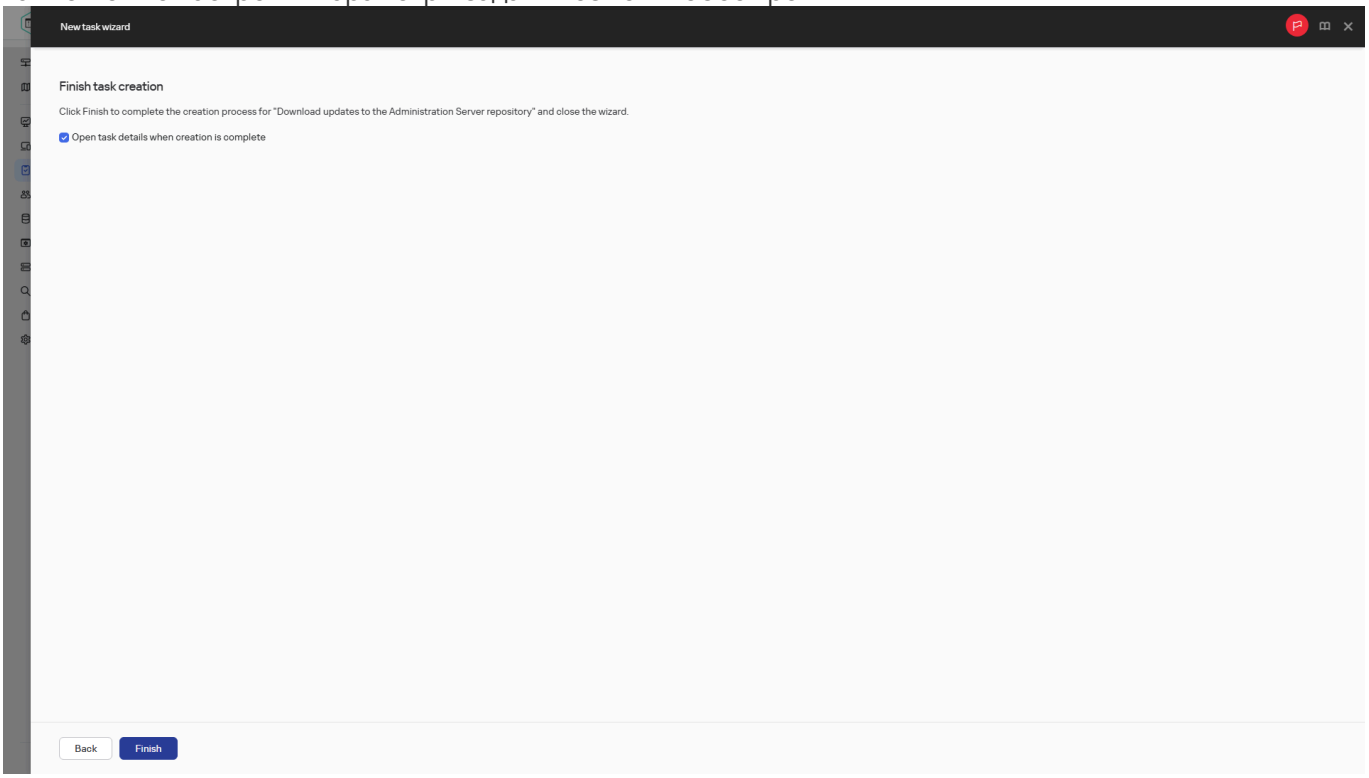
   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Security Center выберите тип задачи **Загрузка обновлений в хранилище Сервера администрирования**.

4. Укажите название задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).



Создание задачи Загрузка обновлений в хранилище Сервера администрирования

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.



Завершение создания задачи

6. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.

7. Чтобы открыть окно свойств задачи, нажмите на имя созданной задачи.

8. В окне свойств задачи на вкладке **Параметры приложения** укажите следующие параметры:

Источники обновлений

В качестве источника обновлений можно использовать:

- Серверы обновлений "Лаборатории Касперского" (выбрано по умолчанию).
- Главный Сервер администрирования

  Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.

- Локальная или сетевая папка

  Локальная или сетевая папка, которая содержит последние обновления. Сетевая папка может быть FTP-сервером, HTTP-сервером или общим ресурсом SMB.

  При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования. Путь к папке зависит от операционной системы устройства. Поскольку локальная папка расположена на Сервере администрирования с операционной системой Linux, вам нужно указать POSIX-путь, например, /path/to/dir.

  При выборе сетевой папки SMB в качестве источника обновлений смонтируйте папку на устройстве, где установлен Сервер администрирования, прежде чем выбирать эту папку. Затем укажите путь к смонтированной папке, используя путь к ее локальной файловой системе. Доступ к папке осуществляется с использованием SMB-протокола.

  > Локальная или сетевая папка, а также FTP- или HTTP-сервер, используемый в качестве источника обновлений, должны содержать структуру папок, соответствующую структуре папок на серверах обновлений "Лаборатории Касперского". Вы можете получить эту структуру с помощью утилиты Kaspersky Update Utility.

> 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 Linux 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.

Принудительно обновить подчиненные Серверы

Если параметр включен, Сервер администрирования будет запускать задачи получения обновлений на подчиненных Серверах администрирования сразу после получения обновлений. Задачи обновления запускаются с использованием источника обновления, который настроен в свойствах задачи на подчиненных Серверах администрирования.

Если этот параметр выключен, задачи обновления на подчиненных Серверах администрирования начинаются в соответствии с расписанием.

По умолчанию параметр выключен.

Копировать полученные обновления в дополнительные папки

Если флажок установлен, после получения обновлений Сервер администрирования будет копировать обновления в указанные папки. Используйте этот параметр, если хотите управлять вручную обновлениями на вашем устройстве.

Например, вы можете использовать этот параметр в следующей ситуации: сеть организации содержит несколько независимых подсетей и устройства из каждой подсети не имеют доступ к другой подсети. При этом устройства во всех подсетях имеют доступ к общей сетевой папке. В этом случае для Сервера администрирования в одной из подсетей укажите загрузку обновлений с серверов обновлений "Лаборатории Касперского", включите этот параметр и укажите эту сетевую папку. В задаче загрузка обновлений в хранилище для Сервера администрирования укажите эту же сетевую папку в качестве источника обновлений.

Если вы выберете копирование загруженных обновлений в локальную папку, необходимо указать на устройстве папку, которая содержит установленный Сервер администрирования. Путь к папке зависит от операционной системы устройства. Поскольку локальная папка расположена на Сервере администрирования с операционной системой Linux, вам нужно указать POSIX-путь, например, /path/to/dir.

При выборе сетевой папки, расположенной на Сервере администрирования с операционной системой Linux, нужно заранее обеспечить доступ к сетевой папке с устройства, на котором установлен Сервер администрирования, смонтировав папку. Доступ к папке осуществляется с использованием SMB-протокола.

По умолчанию параметр выключен.

Скачать файлы различий

Этот параметр включает функцию загрузки файлов различий.

По умолчанию параметр выключен.

Скачивать обновления, используя старую схему

Начиная с версии 14, Kaspersky Security Center загружает обновления баз и модулей приложений по новой схеме. Чтобы приложение могло 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 **Скачивать 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 приложений:

- 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 **Скачивать 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.

Скачать файл запроса на обновление автоматически

Если вы хотите, чтобы утилита Kaspersky Update Utility скачивала только необходимые обновления с подходящей конфигурацией, включите этот параметр и укажите путь, где Kaspersky Security Center Linux создаст файл запроса на обновление с информацией о скачанных обновлениях. Файл запроса на обновление содержит временную метку и MD5-хеш для контроля версий.

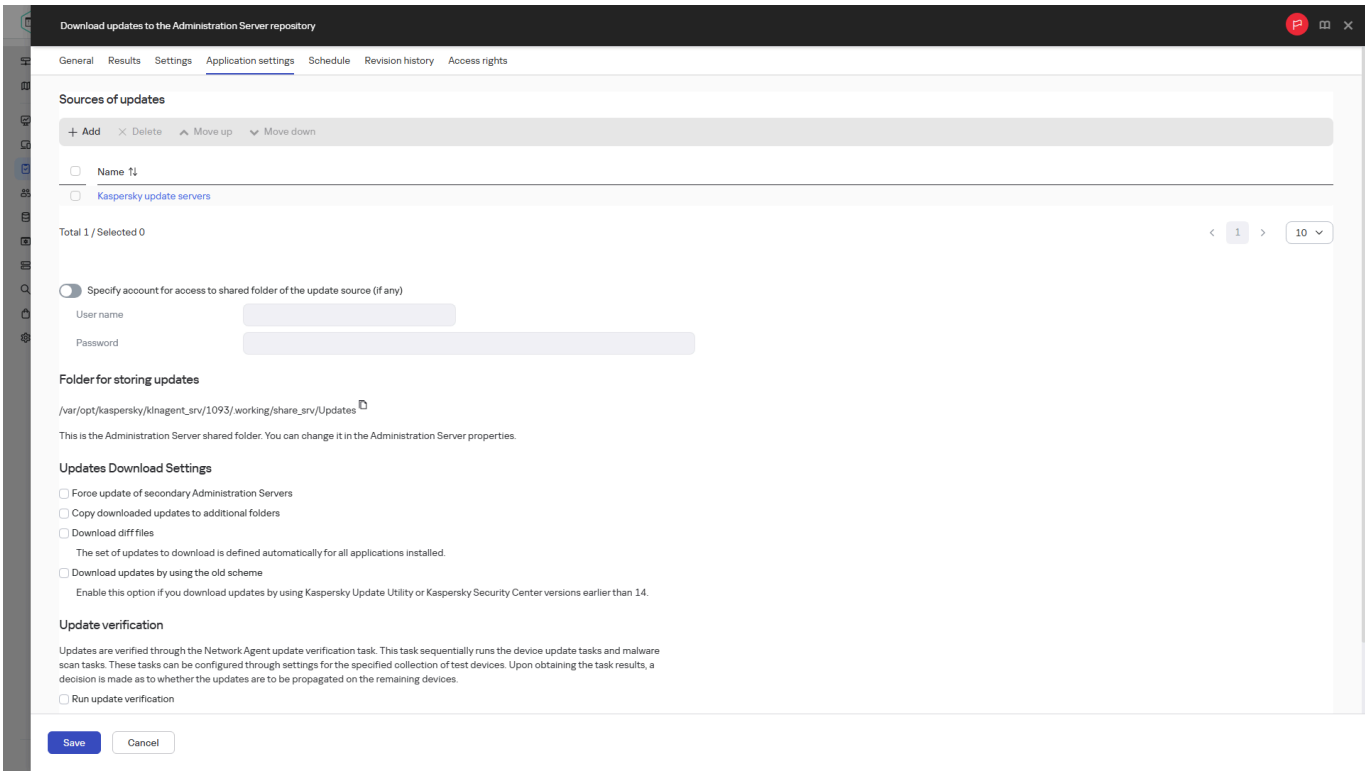
Убедитесь, что параметр **Скачивать обновления, используя старую схему** выключен.

Загрузка обновлений в Kaspersky Update Utility также должна быть настроена.

По умолчанию указан следующий путь: /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/retranslation_request.xml. При необходимости вы можете изменить имя по умолчанию (retranslation_request) и путь.

Файл запроса может быть размещен в локальной папке или в папке общего доступа. При использовании папки общего доступа вам нужно 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 выполнении задачи *Загрузка обновлений в хранилище задачи Сервера администрирования* Kaspersky Security Center Linux создает файл запроса на обновление в формате .xml по указанному вами пути. Утилита Kaspersky Update Utility автоматически получает информацию из файла запроса, а затем скачивает только необходимые обновления. Если утилита Kaspersky Update Utility не может получить информацию автоматически (например, у утилиты Kaspersky Update Utility нет доступа к папке, где приложение Kaspersky Security Center Linux создало файл запроса), вам нужно передать файл с использованием сторонних инструментов.



Указание свойств задачи загрузки обновлений в хранилище Сервера администрирования

9. В окне свойств задачи на вкладке **Расписание** создайте расписания запуска задачи. При необходимости настройте следующие параметры:

- **Запуск задачи**:

  Вручную (выбрано по умолчанию)

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

  По умолчанию выбран этот вариант.

  Каждые N минут

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

  Каждый N час

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые 6 часов, начиная с текущих системной даты и времени.

  Каждые N дней

  Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются приложением, для которого вы создаете задачу.

По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

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 выбранный день

Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

По умолчанию указано время 18:00 и не выбраны дни месяца.

> Обратите внимание, что вы выбираете порядковый номер дня недели в месяце, а не конкретную дату в месяце или номер недели (первая, вторая неделя месяца). Например, если вы выберите ячейку **Вт** в строке **Первая**, в этом случае задача будет запускаться каждый первый вторник каждого нового месяца.

Вы можете выбрать несколько дней недели.

По завершении другой задачи

Текущая задача будет запущена после завершения другой задачи. Этот параметр работает, только если обе задачи назначены одним и тем же устройствам. Например, вы можете запустить задачу *Управление устройствами* с помощью параметра **Включить устройство** и после ее завершения запустить задачу *Поиск вирусов*, как запускающую задачу.

Вам нужно выбрать запускающую задачу из таблицы и статус, с которым эта задача должна завершиться (**Завершена успешно** или **Сбой**).

При необходимости вы можете искать, сортировать и фильтровать задачи в таблице следующим образом:

- Введите название задачи в поле поиска, чтобы выполнить поиск задачи по названию.
- Нажмите на значок сортировки, чтобы отсортировать задачи по имени.

  По умолчанию задачи отсортированы в алфавитном порядке по возрастанию.
- Нажмите на значок фильтра и в открывшемся окне отфильтруйте задачи по группам, после чего нажмите на кнопку **Применить**.

- Дополнительные параметры задачи:

  Запускать пропущенные задачи

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

Если параметр включен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию. Для расписания **Вручную**, **Один раз** и **Немедленно** задачи выполняются только на тех клиентских устройствах, которые видны в сети. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

По умолчанию параметр включен.

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.

По умолчанию параметр включен.

Использовать автоматическую случайную задержку запуска задачи в интервале

Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

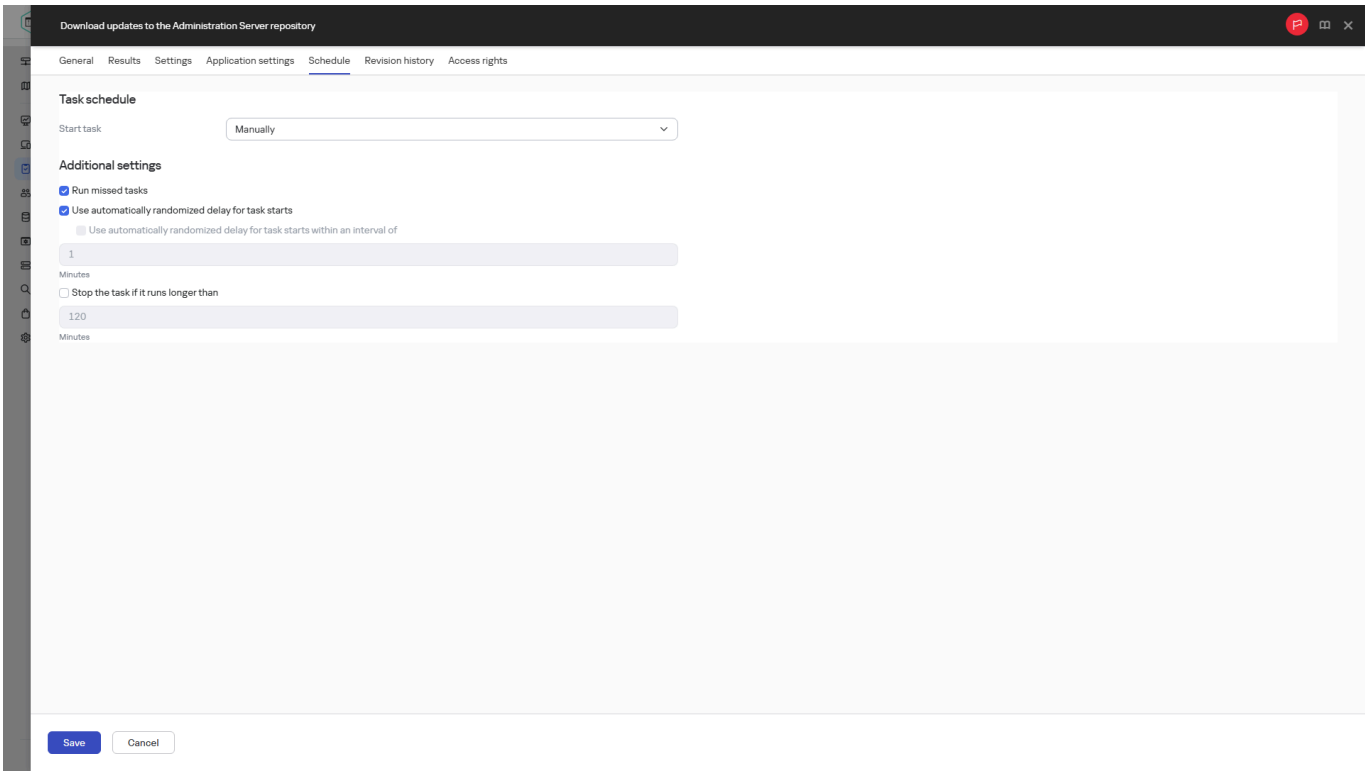
По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

Остановить, если задача выполняется дольше

По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

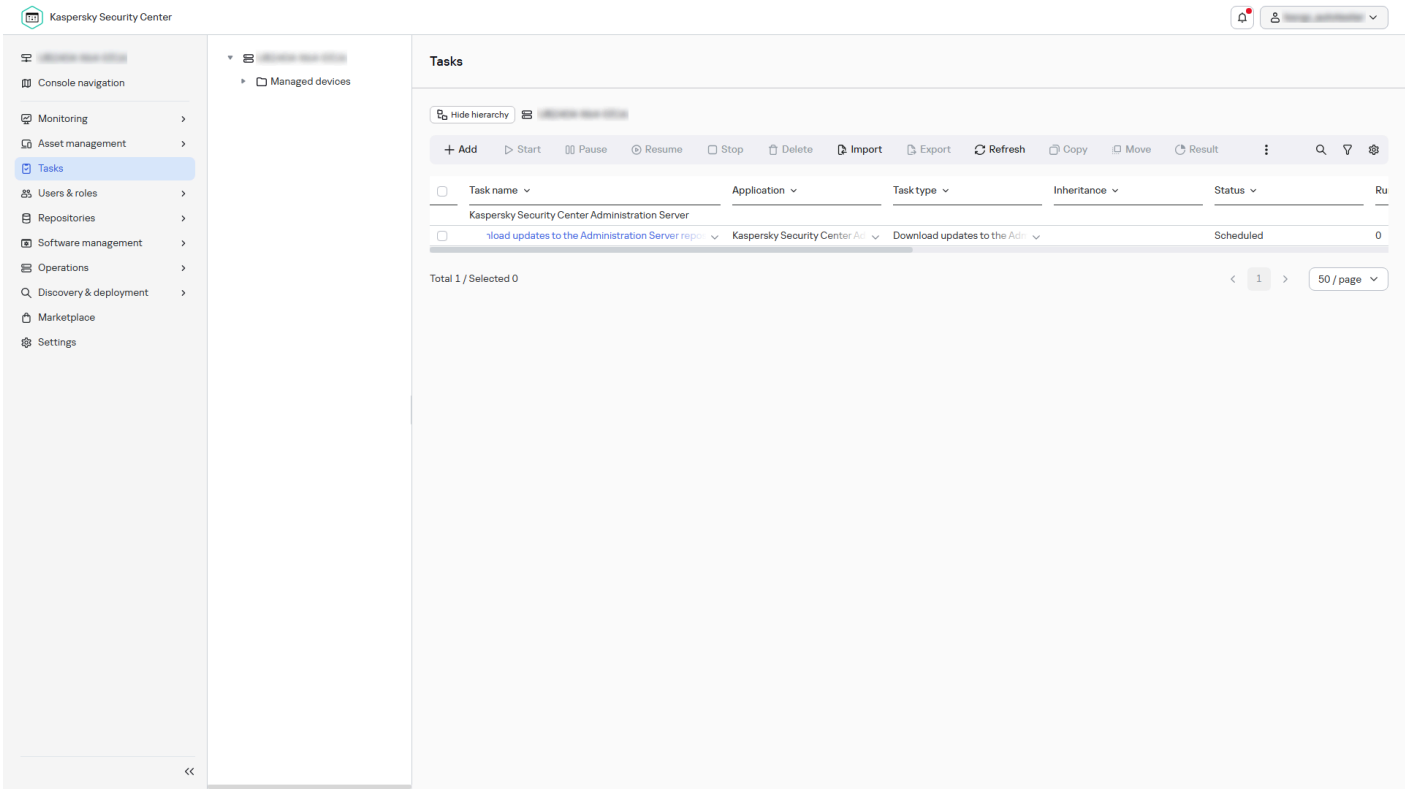
По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.



Указание расписания запуска задачи загрузки обновлений в хранилище Сервера администрирования

10. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.



Список задач

В результате выполнения задачи *Загрузка обновлений в хранилище Сервера администрирования* обновления баз и модули приложений копируются с источника обновлений и размещаются в папке общего доступа Сервера администрирования. Если задача создается для группы администрирования, то она распространяется только на Агенты администрирования, входящие в указанную группу администрирования.

Из папки общего доступа обновления распространяются на клиентские устройства и подчиненные Серверы администрирования.

Проверка полученных обновлений

Перед установкой обновлений на управляемые устройства вы можете сначала проверить их на работоспособность и ошибки с помощью задачи *Проверка обновлений*. Задача *Проверка обновлений* выполняется автоматически в рамках задачи *Загрузка обновлений в хранилище Сервера администрирования*. Сервер администрирования загружает обновления с источника, сохраняет их во временном хранилище и запускает задачу *Проверка обновлений*. В случае успешного выполнения этой задачи обновления копируются из временного хранилища в папку общего доступа Сервера администрирования. Обновления распространяются на клиентские устройства, для которых Сервер администрирования является источником обновления.

Если по результатам выполнения задачи *Проверка обновлений* размещенные во временном хранилище обновления признаны некорректными или задача завершается с ошибкой, копирование обновлений в папку общего доступа не производится. На Сервере администрирования остается предыдущий набор обновлений. Запуск задач с типом расписания **При загрузке обновлений в хранилище** также не выполняется. Эти операции выполняются при следующем запуске задачи *Загрузка обновлений в хранилище Сервера администрирования*, если проверка нового набора обновлений завершится успешно.

Набор обновлений считается некорректным, если хотя бы на одном из тестовых устройств выполняется одно из следующих условий:

- произошла ошибка выполнения задачи обновления;
- после применения обновлений изменился статус постоянной защиты приложения безопасности;
- в ходе выполнения задачи проверки по требованию был найден зараженный объект;
- произошла ошибка функционирования приложения "Лаборатории Касперского".

Если ни одно из перечисленных условий ни на одном из тестовых устройств не выполняется, набор обновлений признается корректным и задача *Проверка обновлений* считается успешно выполненной.

Прежде чем приступить к созданию задачи *Проверка обновлений*, выполните предварительные условия:

1. Создайте группу администрирования с несколькими тестовыми устройствами. Эта группа понадобится вам для проверки обновлений.

   В качестве тестовых устройств рекомендуется использовать хорошо защищенные устройства с наиболее распространенной в сети организации программной конфигурацией. Такой подход повышает качество и вероятность обнаружения вирусов при проверке, а также минимизирует риск ложных срабатываний. При нахождении вирусов на тестовых устройствах задача *Проверка обновлений* считается завершившейся неудачно.

2. Создайте задачи обновления и поиска вредоносного ПО для какого-нибудь приложения, которое поддерживает Kaspersky Security Center Linux, например, Kaspersky Endpoint Security для Linux. При создании задач обновления и поиска вредоносного ПО укажите группу администрирования с тестовыми устройствами.

   Задача *Проверка обновлений* последовательно запускает задачи обновления и поиска вредоносного ПО на тестовых устройствах, чтобы убедиться, что все обновления актуальны. Также при создании задачи *Проверка обновлений* необходимо указать задачи обновления и поиска вредоносного ПО.

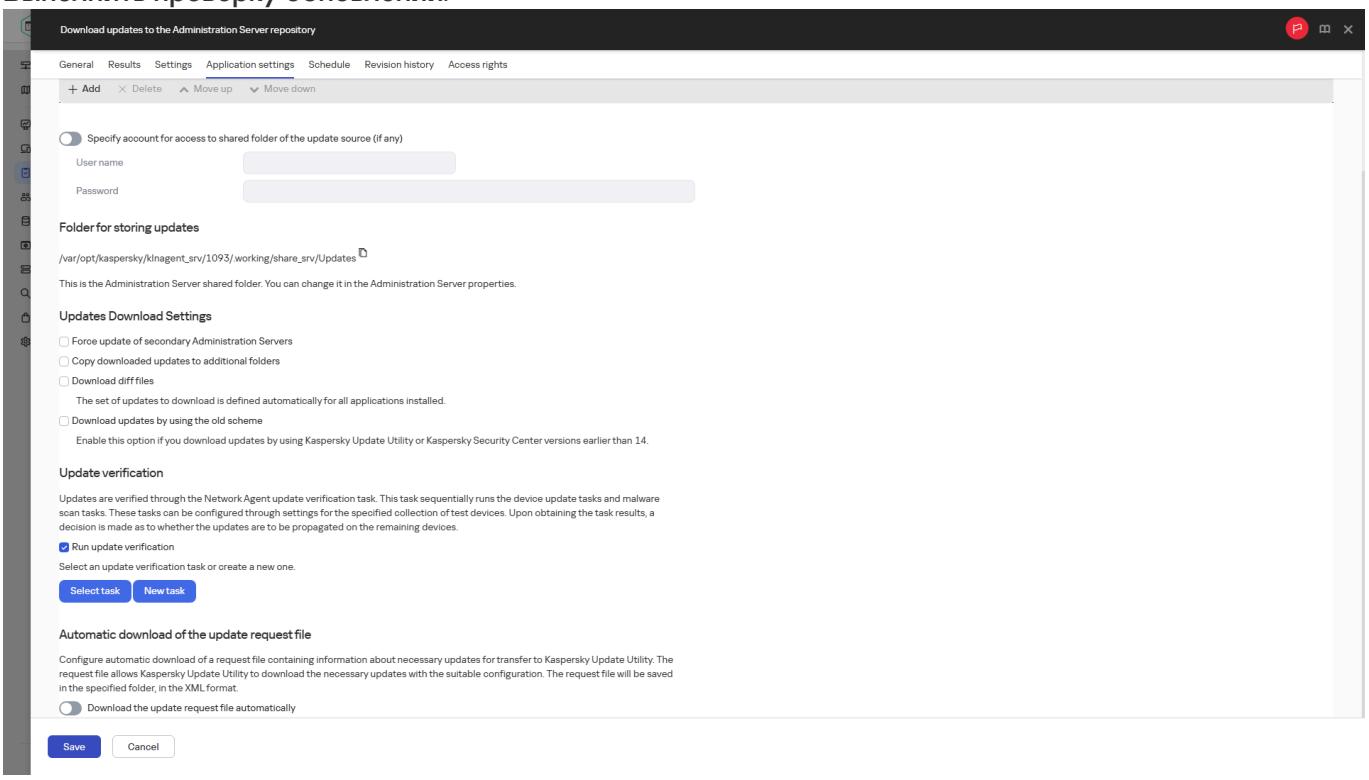
3. Создайте задачу *Загрузка обновлений в хранилище Сервера администрирования*.

Чтобы Kaspersky Security Center Linux проверял полученные обновления перед распространением их на клиентские устройства:

1. В главном окне приложения перейдите в раздел **Задачи**.

2. Нажмите на название задачи **Загрузка обновлений в хранилище Сервера администрирования**.

3. В открывшемся окне свойств задачи перейдите на вкладку **Параметры приложения** и включите параметр **Выполнить проверку обновлений**.



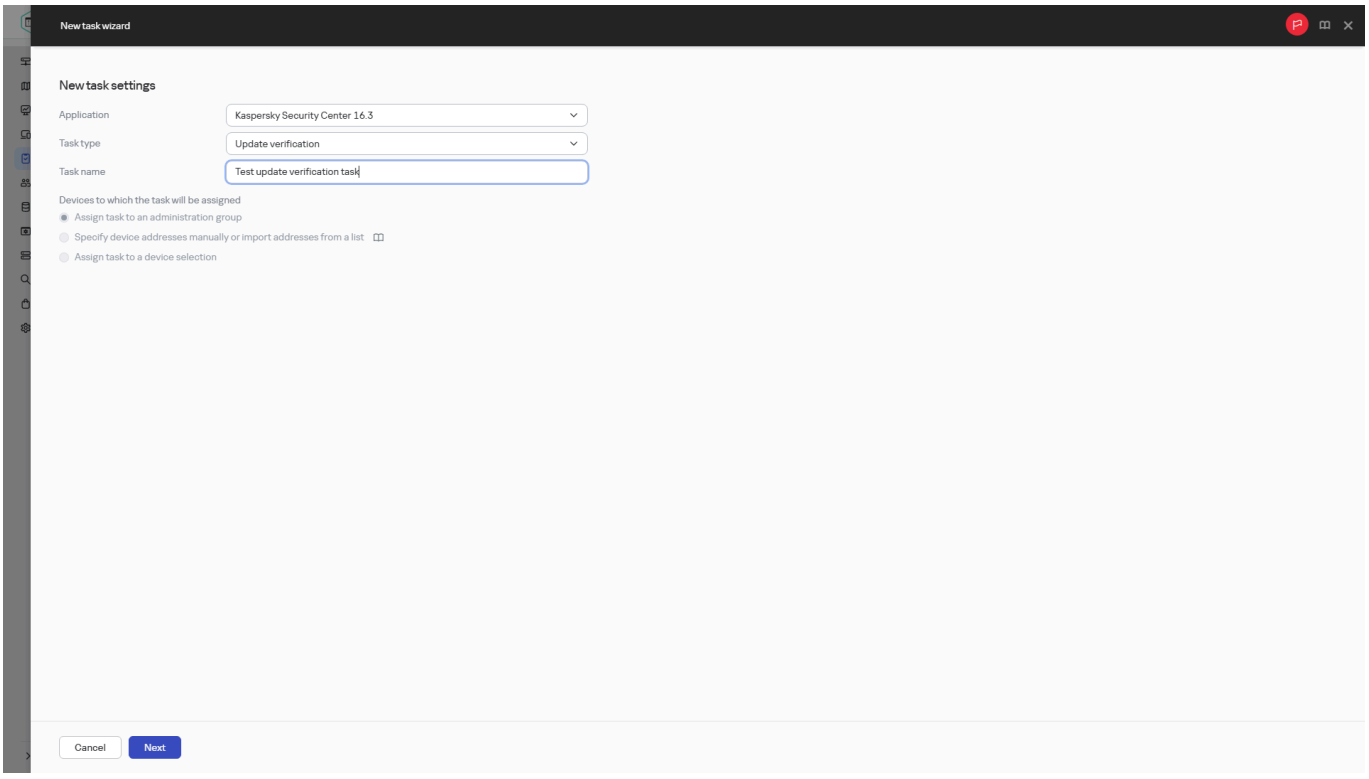
Параметры задачи Загрузка обновлений в хранилище Сервера администрирования

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**.

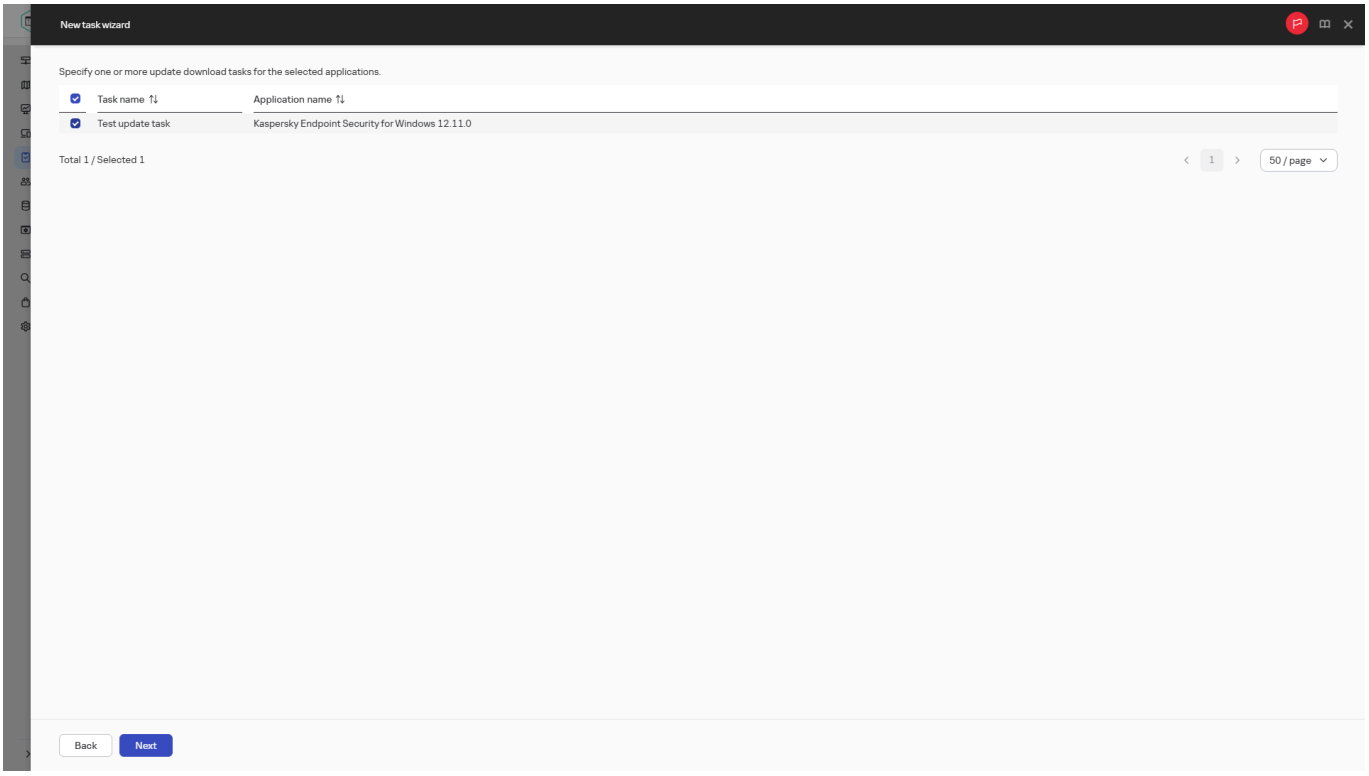
   b. В открывшемся мастере создания задачи укажите название задачи, если вы хотите изменить предустановленное имя.



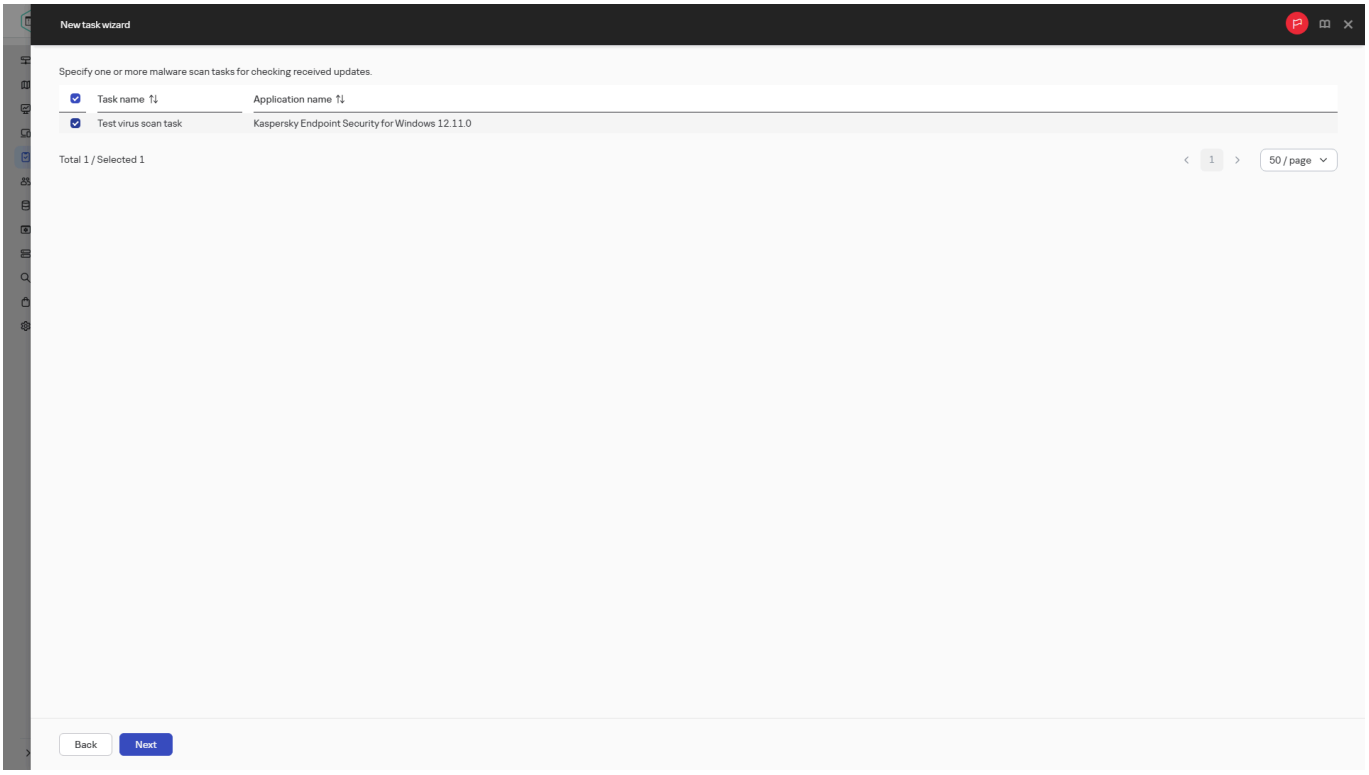
Создание задачи проверки обновлений

   a. Выберите созданную ранее группу администрирования с тестовыми устройствами.

   b. Выберите задачу обновления необходимого приложения, которое поддерживается Kaspersky Security Center Linux.



a. Выберите задачу поиска вредоносного ПО для необходимого приложения, поддерживаемого Kaspersky Security Center Linux.



Выбор задачи поиска вредоносного ПО

После этого появляются следующие параметры. Рекомендуется оставить их включенными:

Перезагружать устройство после обновления баз

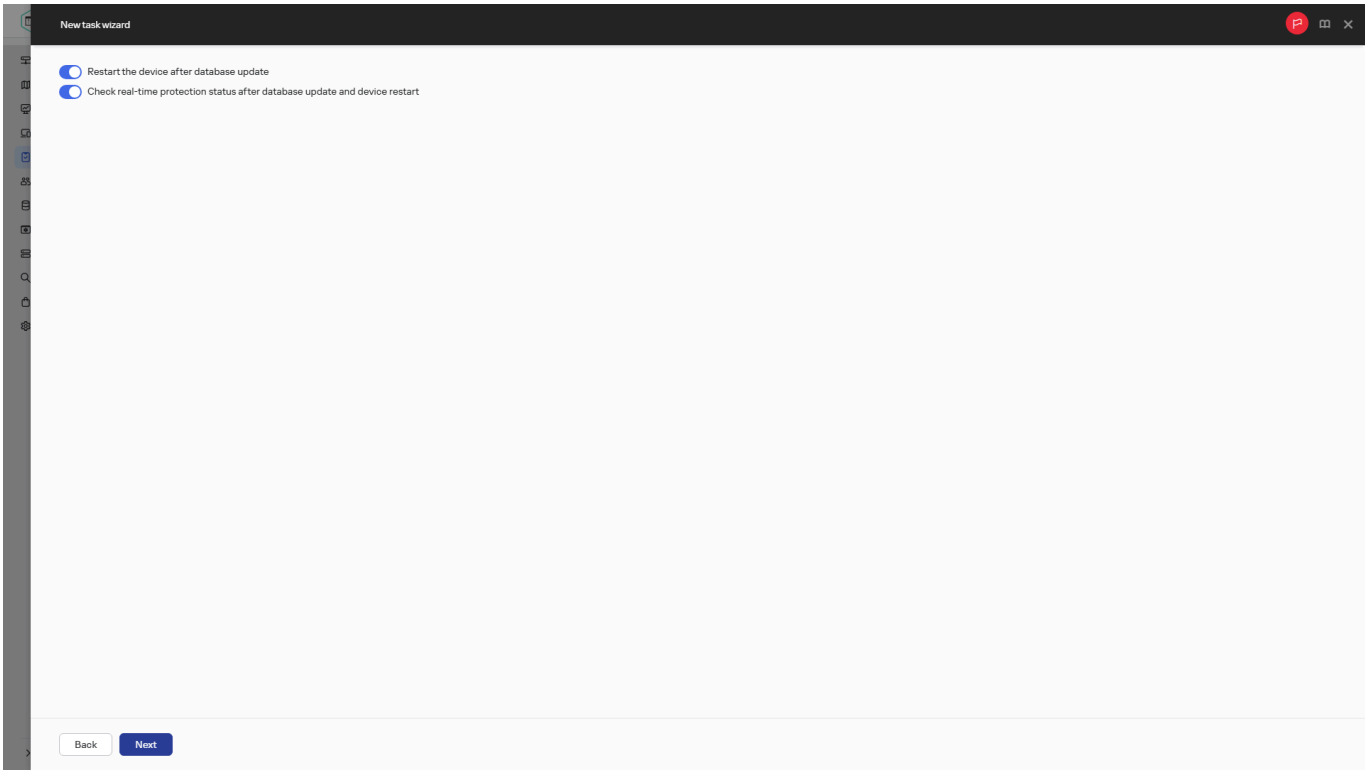
После обновления антивирусных баз на устройстве рекомендуется перезагрузить устройство.

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.



Указание параметров задачи

a. 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.

Создание задачи загрузки обновлений в хранилища точек распространения

Вы можете создать задачу *Загрузка обновлений в хранилища точек распространения* для группы администрирования. Такая задача будет выполняться для точек распространения, входящих в указанную группу администрирования.

Вы можете использовать эту задачу, например, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.

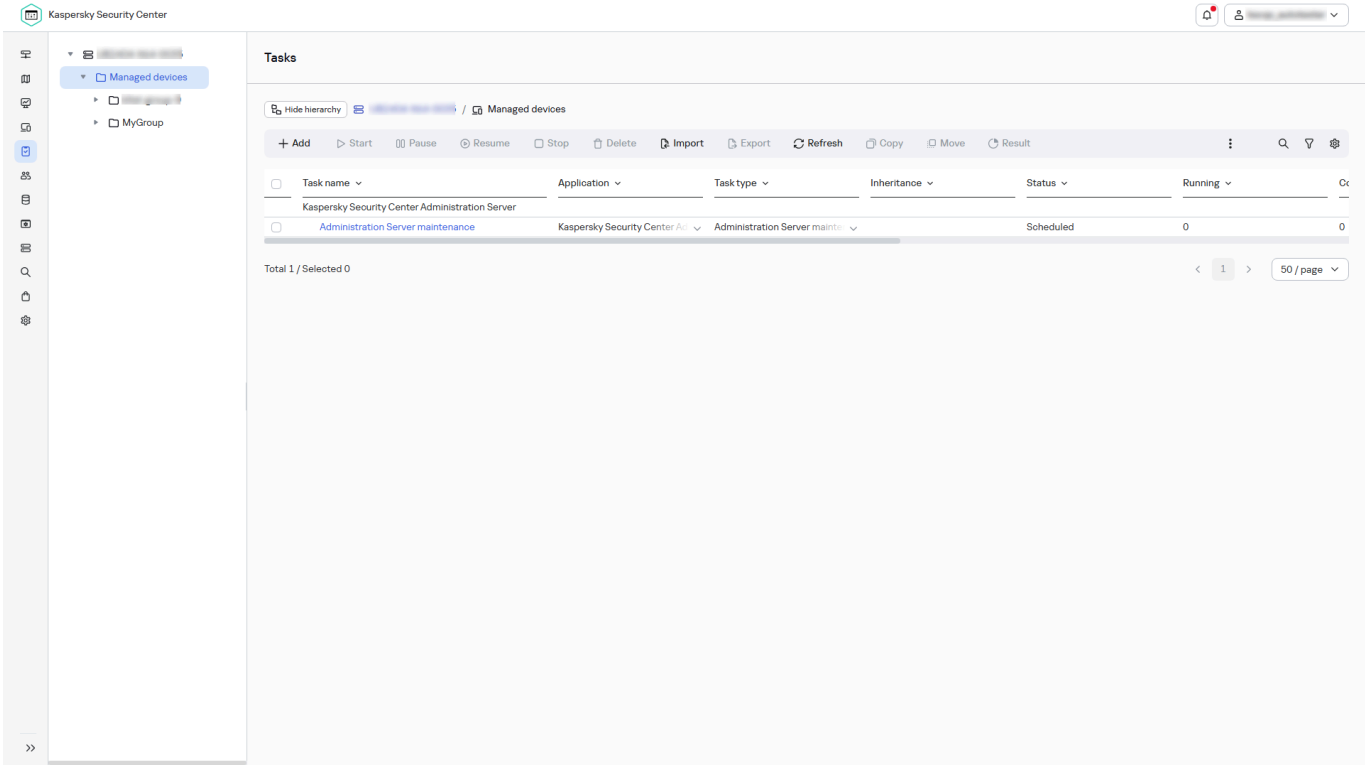
Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилища точек распространения. Список обновлений включает:

- обновления баз и модулей приложений для приложений безопасности "Лаборатории Касперского";
- обновления компонентов Kaspersky Security Center;
- обновления приложений безопасности "Лаборатории Касперского".

После загрузки обновлений их можно распространять на управляемые устройства.

*Чтобы создать задачу **Загрузка обновлений в хранилища точек распространения** для выбранной группы администрирования:*

1. В главном окне приложения перейдите в раздел **Задачи**.



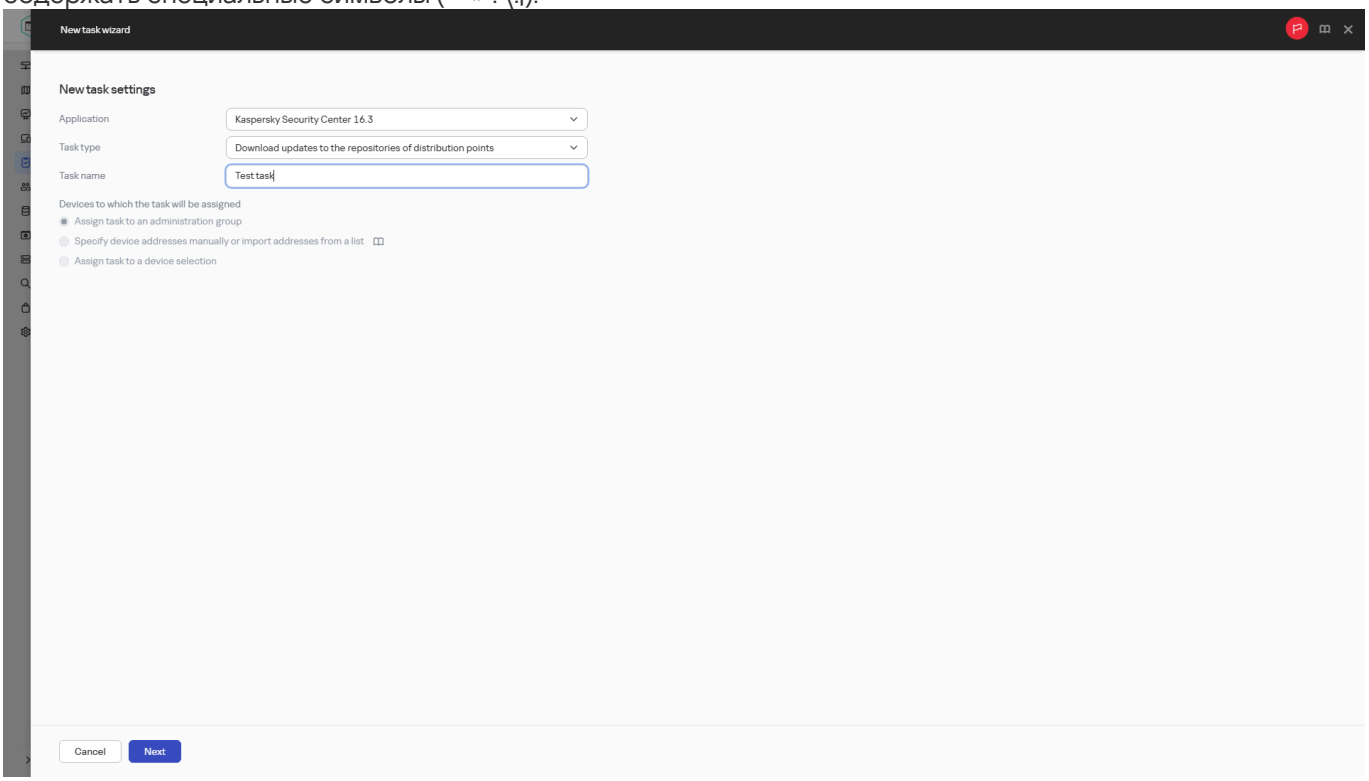
Раздел Задачи

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

3. Для приложения Kaspersky Security Center выберите в поле **Тип задачи** выберите **Загрузка обновлений в хранилища точек распространения**.

4. Укажите название задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).



Создание задачи Загрузка обновлений в хранилища точек распространения

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 вкладке **Параметры приложения** окна свойств задачи укажите следующие параметры:

   Источники обновлений

   В качестве источника обновлений для точки распространения могут быть использованы следующие ресурсы:

   - Серверы обновлений "Лаборатории Касперского"

     HTTP-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложения.

     По умолчанию этот вариант выбран.

   - Локальная или сетевая папка

     Локальная или сетевая папка, которая содержит последние обновления. В качестве сетевой папки можно использовать только смонтированную общую папку SMB. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

В задачах *Загружать обновления в хранилище Сервера администрирования* и *Загружать обновления в хранилища точек распространения* аутентификация пользователя не работает, если в качестве источника обновлений выбрана защищенная паролем локальная или сетевая папка. Чтобы решить эту проблему, сначала смонтируйте защищенную паролем папку, а затем укажите необходимые учетные данные, например, средствами операционной системы. После этого вы можете выбрать эту папку в качестве источника обновлений в задаче загрузки обновлений. Kaspersky Security Center Linux 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.

Скачать файлы различий

Этот параметр включает функцию загрузки файлов различий.

По умолчанию параметр выключен.

Скачивать обновления, используя старую схему

Начиная с версии 14, Kaspersky Security Center загружает обновления баз и модулей приложений по новой схеме. Чтобы приложение могло 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 **Скачивать 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 приложений:

- 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 **Скачивать 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 задачи**:

  Вручную (выбрано по умолчанию)

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

  По умолчанию выбран этот вариант.

  Каждые N минут

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

Каждый N час

Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

По умолчанию задача запускается каждые 6 часов, начиная с текущих системной даты и времени.

Каждые N дней

Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются приложением, для которого вы создаете задачу.

По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

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 выбранный день

Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

По умолчанию указано время 18:00 и не выбраны дни месяца.

> Обратите внимание, что вы выбираете порядковый номер дня недели в месяце, а не конкретную дату в месяце или номер недели (первая, вторая неделя месяца). Например, если вы выберите ячейку **Вт** в строке **Первая**, в этом случае задача будет запускаться каждый первый вторник каждого нового месяца.

Вы можете выбрать несколько дней недели.

При обнаружении вирусной атаки

Запускать задачу после возникновения события *Вирусная атака*. Выберите типы приложений, которые будут отслеживать вирусные атаки. Доступны следующие типы приложений:

- антивирусы для рабочих станций и файловых серверов;
- антивирусы защиты периметра;
- антивирусы для почтовых систем.

По умолчанию выбраны все типы приложений.

Вы можете запускать разные задачи в зависимости от типа приложения безопасности, сообщающего о вирусной атаке. В этом случае удалите выбор типов приложений, которые вам не нужны.

По завершении другой задачи

Текущая задача будет запущена после завершения другой задачи. Этот параметр работает, только если обе задачи назначены одним и тем же устройствам. Например, вы можете запустить задачу *Управление устройствами* с помощью параметра **Включить устройство** и после ее завершения запустить задачу *Поиск вирусов*, как запускающую задачу.

Вам нужно выбрать запускающую задачу из таблицы и статус, с которым эта задача должна завершиться (**Завершена успешно** или **Сбой**).

При необходимости вы можете искать, сортировать и фильтровать задачи в таблице следующим образом:

- Введите название задачи в поле поиска, чтобы выполнить поиск задачи по названию.
- Нажмите на значок сортировки, чтобы отсортировать задачи по имени.

  По умолчанию задачи отсортированы в алфавитном порядке по возрастанию.
- Нажмите на значок фильтра и в открывшемся окне отфильтруйте задачи по группам, после чего нажмите на кнопку **Применить**.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию. Для расписания **Вручную**, **Один раз** и **Немедленно** задачи выполняются только на тех клиентских устройствах, которые видны в сети. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **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.

  По умолчанию параметр включен.

- **Использовать автоматическую случайную задержку запуска задачи в интервале**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

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 модулей приложений 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.

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 Linux 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.

При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования. Путь к папке зависит от операционной системы устройства. Поскольку локальная папка расположена на Сервере администрирования с операционной системой Linux, вам нужно указать POSIX-путь, например, /path/to/dir.

В качестве сетевой папки можно использовать только смонтированную общую папку 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.

Чтобы добавить источники обновлений:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Загрузка обновлений в хранилище Сервера администрирования**.
3. Перейдите на вкладку **Параметры приложения**.
4. В таблице **Источники обновлений** нажмите на кнопку **Добавить**.
5. В открывшемся окне добавьте нужные источники обновлений и нажмите на кнопку **Сохранить**.

   Если вы установите флажок **Локальная или сетевая папка**, укажите путь к папке.
6. Нажмите на кнопку **Сохранить** в окне задач.

Теперь обновления загружаются в хранилище Сервера администрирования из указанных источников.

Если вы добавляете и серверы обновлений "Лаборатории Касперского", и локальную или сетевую папку, вы можете установить приоритеты для обновлений. Для этого в таблице **Источники обновлений** установите флажок рядом с обновлением, для которого вы хотите изменить приоритет и нажмите на кнопку **Вверх** или **Вниз**.

Одобрение и отклонение обновлений программного обеспечения

Параметры задачи установки обновлений могут требовать одобрения обновлений, которые должны быть установлены. Вы можете подтверждать обновления, которые необходимо установить, и отклонять обновления, которые не должны быть установлены.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом установить эти обновления на клиентские устройства.

Одобрение и отклонение обновлений доступно только для Агента администрирования и управляемых приложений, установленных на клиентских устройствах под управлением Windows. Бесшовное обновление Сервера администрирования, Kaspersky Security Center Web Console и веб-плагинов управления не поддерживается. Для обновления этих компонентов вам необходимо скачать их последние версии с сайта "Лаборатории Касперского" и установить их вручную.

Чтобы подтвердить или отменить одно или несколько обновлений:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Приложения "Лаборатории Касперского" → Бесшовные обновления**.

   Отобразится список доступных обновлений.

Для обновлений управляемых приложений может потребоваться установка определенной минимальной версии Kaspersky Security Center. Если эта версия более поздняя, чем ваша текущая, эти обновления отображаются, но не могут быть одобрены. Также из таких обновлений невозможно создать инсталляционные пакеты, пока вы не обновите Kaspersky Security Center. Вам будет предложено обновить ваш экземпляр Kaspersky Security Center до необходимой минимальной версии.

2. При необходимости примите Лицензионное соглашение, нажав на кнопку **Просмотреть и принять Лицензионные соглашения**.

3. Выберите обновления, которые требуется подтвердить или отклонить.

4. Нажмите на кнопку **Одобрить**, чтобы одобрить выбранное обновление, или **Отклонить**, чтобы отклонить выбранное обновление.

   По умолчанию установлено значение *Не определено*.

Обновления, для которых вы установили статус *Одобрено*, помещаются в очередь на установку.

Обновления, для которых вы установили статус *Отклонено*, деинсталлируются (если это возможно) с устройств, на которые они были ранее установлены. Также они не будут установлены на устройства позже.

Некоторые обновления для приложений "Лаборатории Касперского" невозможно деинсталлировать. Если вы установили для них статус *Отклонено*, Kaspersky Security Center Linux не будет деинсталлировать эти обновления с устройств, на которые они были установлены ранее. Такие обновления никогда не будут установлены на устройства в будущем.

Если вы устанавливаете статус *Отклонено* для обновлений стороннего программного обеспечения, то эти обновления не будут устанавливаться на те устройства, для которых они были запланированы к установке, но еще не были установлены. Обновления останутся на тех устройствах, на которые они уже были установлены. Если вам потребуется удалить обновления, вы можете сделать это вручную локально.

Автоматическая установка обновлений для Kaspersky Endpoint Security для Windows

Вы можете настроить автоматическое обновление баз и модулей приложения Kaspersky Endpoint Security для Windows на клиентских устройствах.

Чтобы настроить загрузку и автоматическую установку обновлений Kaspersky Endpoint Security для Windows на устройства:

1. В главном окне приложения перейдите в раздел **Задачи**.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

3. Для приложения Kaspersky Endpoint Security для Windows выберите подтип задачи **Обновление**.

4. Укажите название задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

5. Выберите область действия задачи.

6. Укажите группу администрирования, выборку устройств или устройства, к которым применяется задача.

7. 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.

8. Нажмите на кнопку **Создать**.

   Задача будет создана и отобразится в списке задач.

9. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

10. В окне свойств задачи обновления на вкладке **Параметры приложения** укажите локальный или мобильный режим:

    - **Локальный режим**: между устройством и Сервером администрирования установлена связь.

    - **Мобильный режим**: между устройством и Kaspersky Security Center Linux не установлена связь (например, если устройство не подключено к интернету).

11. Включите источники обновлений, которые вы хотите использовать для обновления баз и модулей приложения для Kaspersky Endpoint Security для Windows. Если требуется изменить положение источников обновлений в списке, используйте кнопки **Вверх** и **Вниз**. Если включено несколько источников обновлений, Kaspersky Endpoint Security для Windows пытается подключиться к ним один за другим, начиная с верхней части списка, и выполняет задачу обновления, извлекая пакет обновления из первого доступного источника.

12. Включите параметр **Устанавливать одобренные обновления модулей приложений**, чтобы загружать и устанавливать обновления модулей приложений вместе с базами приложений.

    Если параметр включен, то Kaspersky Endpoint Security для Windows уведомляет пользователя о доступных обновлениях модулей приложения и во время выполнения задачи обновления включает обновления модулей приложения в пакет обновлений. Kaspersky Endpoint Security для Windows устанавливает только те обновления, для которых вы установили статус *Одобрено*; обновления будут установлены локально через интерфейс приложения или через Kaspersky Security Center Linux.

    Вы также можете включить параметр **Автоматически устанавливать критические обновления модуля приложения**. При наличии обновлений модулей приложения Kaspersky Endpoint Security для Windows устанавливает обновления со статусом *Предельный* автоматически; остальные обновления модулей приложения – после одобрения их установки администратором.

    Если обновление модулей приложения предполагает ознакомление и согласие с положениями Лицензионного соглашения и Политики конфиденциальности, то приложение устанавливает обновление после согласия пользователя с положениями Лицензионного соглашения и Политики конфиденциальности.

13. Установите флажок **Копировать обновления в папку**, чтобы приложение сохраняло загруженные обновления в папку, а затем укажите путь к папке.

14. Задайте расписание запуска задачи. Чтобы обеспечить своевременное обновление, рекомендуется выбрать вариант **При загрузке обновлений в хранилище**.

15. Нажмите на кнопку **Сохранить**.

При выполнении задачи **Обновление** приложение отправляет запросы серверам обновлений "Лаборатории Касперского".

Некоторые обновления требуют установки последних версий плагинов управляемых приложений.

Об использовании файлов различий для обновления баз и модулей приложений "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 модулями приложения. Использование файлов различий сохраняет трафик внутри сети вашей организации, так как файлы различий занимают меньше места, чем целые файлы баз и модулей приложений. Если функция *Загрузить файлы различий* включена для Сервера администрирования или точки распространения, файлы различий сохраняются на этом Сервере администрирования или точке распространения. В результате устройства, которые получают обновления от этого Сервера администрирования или точки распространения, могут использовать сохраненные файлы различий для обновления своих баз и модулей приложений.

Для оптимизации использования файлов различий рекомендуется синхронизировать расписание обновления устройств с расписанием обновлений Сервера администрирования или точки распространения, с которых это устройство получает обновления. Однако трафик может быть сохранен, даже если устройства обновляются в несколько раз реже, чем Сервер администрирования или точки распространения, с которых устройство получает обновления.

Точки распространения не используют многоадресную IP-рассылку для автоматического распространения файлов различий.

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.

Загрузка обновлений точками распространения

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:

1. В главном окне приложения нажмите на имя 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.

Скачать файлы различий

Этот параметр включает функцию загрузки файлов различий.

По умолчанию параметр включен.

В результате точка распространения будет получать обновления из указанного источника.

Обновление баз и модулей приложений "Лаборатории Касперского" на автономных устройствах

Обновление баз и модулей приложений "Лаборатории Касперского" на управляемых устройствах является важной задачей для обеспечения защиты устройств от вирусов и других угроз. Администратор обычно настраивает регулярное обновление с помощью хранилища Сервера администрирования.

Когда вам необходимо обновить базы данных и модули приложений на устройстве (или группе устройств), которое не подключено к Серверу администрирования (главному или подчиненному), точке распространения или интернету, вам необходимо использовать альтернативные источники обновлений, такие как FTP-сервер или локальная папка. В этом случае вам нужно доставить файлы необходимых обновлений с помощью запоминающего устройства, такого как флеш-накопитель или внешний жесткий диск.

Вы можете скопировать требуемые обновления с:

- Сервера администрирования.

  Чтобы хранилище Сервера администрирования содержало обновления, необходимые для приложения безопасности, установленного на автономном устройстве, по крайней мере на одном из управляемых сетевых устройств должно быть установлено это приложение безопасности. Это приложение должно быть настроено на получение обновлений из хранилища Сервера администрирования с помощью задачи *Загрузка обновлений в хранилище Сервера администрирования*.

- Любого устройства, на котором установлено такое же приложение безопасности и настроено получение обновлений из хранилища Сервера администрирования, хранилища точки распространения или напрямую с серверов обновлений "Лаборатории Касперского".

Ниже приведен пример настройки обновлений баз и модулей приложений путем копирования их из хранилища Сервера администрирования.

Чтобы обновить базы данных и модули приложений "Лаборатории Касперского" на автономных устройствах:

1. Подключите съемный диск к устройству, на котором установлен Сервер администрирования.

2. Скопируйте файлы обновлений на съемный диск.

   По умолчанию обновления расположены:
   /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/Updates/.

   Также вы можете настроить в Kaspersky Security Center Linux регулярное копирование обновлений в выбранную вами папку. Для этого используйте параметр **Копировать полученные обновления в дополнительные папки** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования*. Если вы укажете папку, расположенную на запоминающем устройстве или внешнем жестком диске, в качестве папки назначения для этого параметра, это запоминающее устройство всегда будет содержать последнюю версию обновлений.

3. На автономных устройствах настройте Kaspersky Endpoint Security на получение обновлений из локальной папки или общего ресурса, такого как FTP-сервер или общая папка.

   Инструкции:

   - Справка Kaspersky Endpoint Security для Linux
   - Справка Kaspersky Endpoint Security для Windows

4. Скопируйте файлы обновлений со съемного диска в локальную папку или общий ресурс, который вы хотите использовать в качестве источника обновлений.

5. На автономном устройстве, требующем установки обновлений, запустите задачу Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Windows *Обновление*, в зависимости от операционной системы автономного устройства.

После завершения задачи обновления базы данных и модули приложений "Лаборатории Касперского" будут обновлены на устройстве.

Мониторинг, отчеты и аудит

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 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 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 приложений, передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

   Инструкции:

   - Ограничение максимального количества событий.

8. **Просмотр информации о лицензии**

   Инструкции:

   - Добавление виджета Используемые лицензионные ключи в 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 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 Web Console.

Уведомления

Уведомления предназначены для оповещения о событиях и для того, чтобы помочь вам увеличить скорость ваших ответов на эти события, выполнив рекомендуемые действия, которые вы считаете подходящими.

Срабатывание правил в режиме Интеллектуального обучения

В этом разделе представлена информация об обнаружениях, выполненных правилами Адаптивного контроля аномалий Kaspersky Endpoint Security для Windows на клиентских устройствах.

Правила обнаруживают аномальное поведение на клиентских устройствах и могут блокировать его. Если правила работают в режиме Интеллектуального обучения, они обнаруживают аномальное поведение и отправляют отчеты о каждом таком случае на Сервер администрирования. Вы можете просмотреть отчеты об анализе аномального поведения в разделе **Хранилища → Правила срабатываний в статусе Интеллектуальное обучение**. Вы можете подтвердить обнаружение как корректное или добавить его в исключения, после чего такой тип поведения не будет считаться аномальным.

Информация об обнаружениях хранится в журнале событий на Сервере администрирования (вместе с остальными событиями) и в отчете Адаптивный контроль аномалий.

Подробная информация об Адаптивном контроле аномалий, его правилах, их режимах и статусах приведена в справке Kaspersky Endpoint Security для Windows.

Просмотр и подтверждение обнаружений, выполненных с помощью правил Адаптивного контроля аномалий

Чтобы просмотреть список обнаружений, выполненных с помощью правил Адаптивного контроля аномалий:

1. В главном окне приложения перейдите в раздел **Хранилища → Правила срабатываний в статусе Интеллектуальное обучение**.

   В списке отображается следующая информация об обнаружении, выполняемая с помощью правил Адаптивного контроля аномалий:

   - **Группа администрирования**

     Имя группы администрирования, в которую включено устройство.

   - **Виртуальный Сервер администрирования**

     Виртуальный Сервер администрирования, который управляет устройством.

   - **Имя устройства**

     Имя клиентского устройства, на котором было применено правило.

   - **Имя**

     Имя правила, которое было применено.

   - **Статус**

     Исключение – если администратор обработал это обнаружение и добавил его как исключение из правил. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

     Подтверждение – если администратор обработал это обнаружение и подтвердил его. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

     Пусто – если администратор не обработал обнаружение.

   - **Количество обнаружений**

     Количество обнаружений одного эвристического правила, одного процесса и одного клиентского устройства. Это количество рассчитано Kaspersky Endpoint Security.

- **Имя пользователя**

  Имя пользователя клиентского устройства, запустившего процесс, который сгенерировал обнаружение.

- **Путь исходного процесса**

  Путь к исходному процессу, то есть к процессу, выполнившему действие (подобную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного процесса**

  Хеш SHA256 исходного файла процесса (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь исходного объекта**

  Путь к объекту, который запустил процесс (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного объекта**

  Хеш SHA256 исходного файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого процесса**

  Путь к целевому процессу (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого процесса**

  Хеш SHA256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого объекта**

  Путь к целевому объекту (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого объекта**

  Хеш SHA256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Обработан**

  Дата обнаружения аномалии.

Чтобы просмотреть свойства обнаружения:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Правила срабатываний в статусе Интеллектуальное обучение**.

2. Выполните одно из следующих действий:

   - В столбце **Имя** нажмите на ссылку с названием обнаружения, которое вы хотите просмотреть.

   - В списке обнаружений установите флажки рядом с уязвимостями, которые вы хотите просмотреть и нажмите на кнопку **Свойства**.

Откроется окно свойств выбранного обнаружения.

Вы можете подтвердить любое обнаружение из списка обнаружений правил Адаптивного контроля аномалий или в окне свойств выбранного обнаружения.

Чтобы подтвердить обнаружение:

- Выберите одно или несколько обнаружений в списке обнаружений и нажмите на кнопку **Подтвердить**.
- Откройте окно свойств выбранного обнаружения и нажмите на кнопку **Подтвердить**.

Статус обнаружения изменится на **Подтверждение**. Обнаружение исчезнет из списка обнаружений после следующей синхронизации клиентского устройства с Сервером администрирования.

Ваше подтверждение влияет на статистику, используемую правилами. Дополнительную информацию см. в справке Kaspersky Endpoint Security для Windows.

Добавление исключений в правила Адаптивного контроля аномалий

Мастер добавления в исключения Адаптивного контроля аномалий позволяет добавлять исключения из правил Адаптивного контроля аномалий для Kaspersky Endpoint Security.

Чтобы добавить исключения из правил Адаптивного контроля аномалий с помощью мастера:

1. Запустите мастер одним из следующих способов:

   - В главном окне приложения перейдите в раздел **Хранилища** → **Правила срабатываний в статусе Интеллектуальное обучение**, выберите одно или несколько обнаружений и нажмите на кнопку **Исключить**.

     За один раз можно добавить до 1000 исключений.

     Перед добавлением обнаружения в исключения вы можете просмотреть свойства обнаружения, нажав на имя обнаружения или на кнопку **Свойства**. В открывшемся окне свойств обнаружения вы также можете нажать на кнопку **Исключить**.

   - В главном окне приложения перейдите в раздел **Мониторинг** → **Выборки событий**, нажмите на ссылку с нужной выборкой событий, установите флажок рядом с обнаружением, которое вы хотите исключить, и нажмите на кнопку **Исключить из Адаптивного контроля аномалий**.

   Запустится мастер добавления в исключения Адаптивного контроля аномалий. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. Выберите политики и профили политик, в которые вы хотите добавить исключения.

   Унаследованные политики не могут быть обновлены. Если у вас нет прав на изменение политики, такая политика не будет обновлена.

3. Нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Статус обнаружения изменится на **Исключение**. Обнаружение исчезнет из списка обнаружений после следующей синхронизации клиентского устройства с Сервером администрирования. Исключение из правил Адаптивного контроля аномалий настроено и применено.

Панель мониторинга и виджеты

В этом разделе содержится информация о панели мониторинга и виджетах, представленных в панели мониторинга. Раздел содержит инструкции по управлению виджетами и настройке 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 Web Console в разделе **Мониторинг → Панель мониторинга**.

В панели мониторинга представлены настраиваемые виджеты. Вы можете выбрать большое количество различных виджетов, представленных в виде круговых диаграмм, таблиц, графиков, гистограмм и списков. Информация, отображаемая в виджетах, обновляется автоматически, период обновления составляет от одной до двух минут. Интервал времени между обновлениями зависит от типа виджета. Вы можете обновить данные виджета вручную с помощью меню, в любое время.

По умолчанию виджеты включают информацию о событиях, хранящихся в базе данных Сервера администрирования.

Kaspersky Security Center Web Console имеет по умолчанию набор виджетов для следующих категорий:

- **Состояние защиты**
- **Развертывание**
- **Обновление**
- **Статистика угроз**
- **Другие**

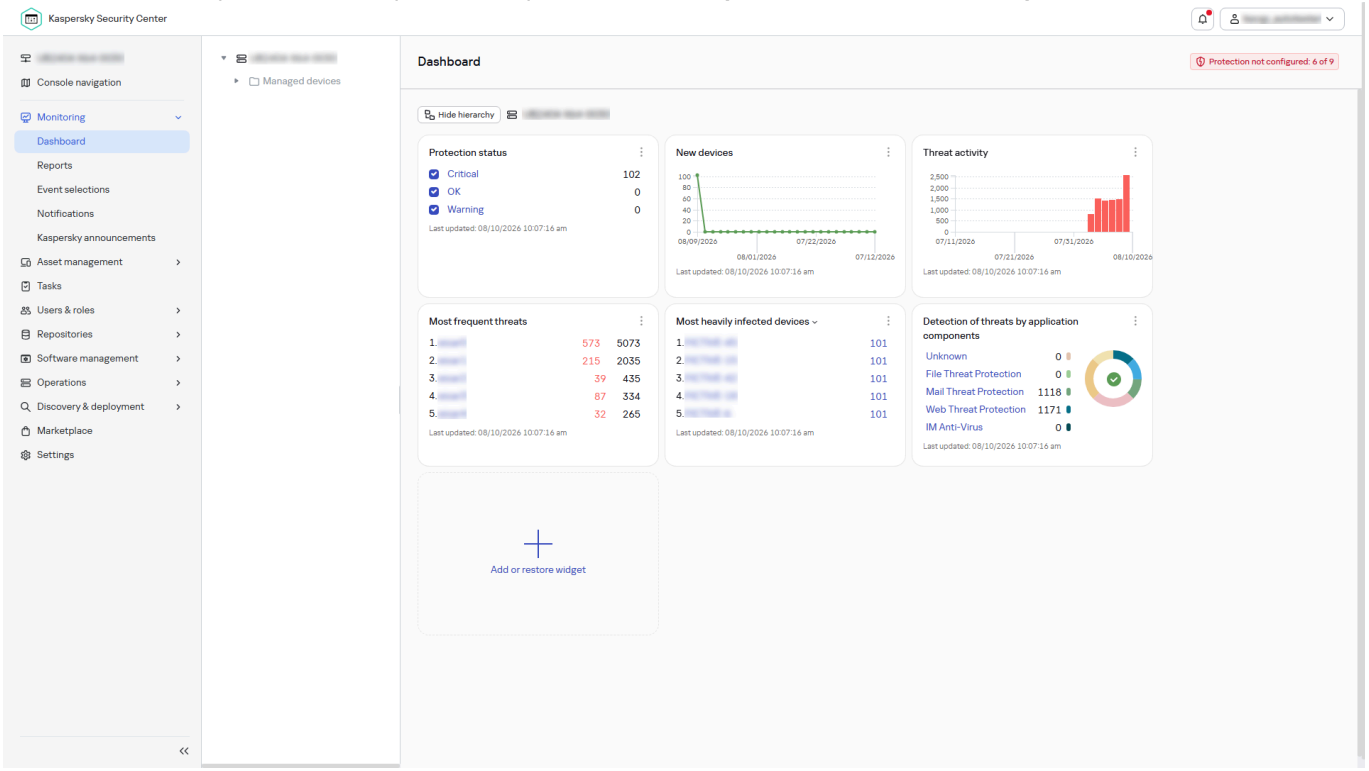
Некоторые виджеты имеют текст со ссылками. Чтобы просмотреть подробную информацию, перейдите по ссылке.

При настройке панели мониторинга можно добавлять необходимые виджеты, скрывать виджеты, а также менять внешний вид или размер виджетов, перемещать виджеты и изменять параметры виджетов.

Добавление виджета на информационную панель

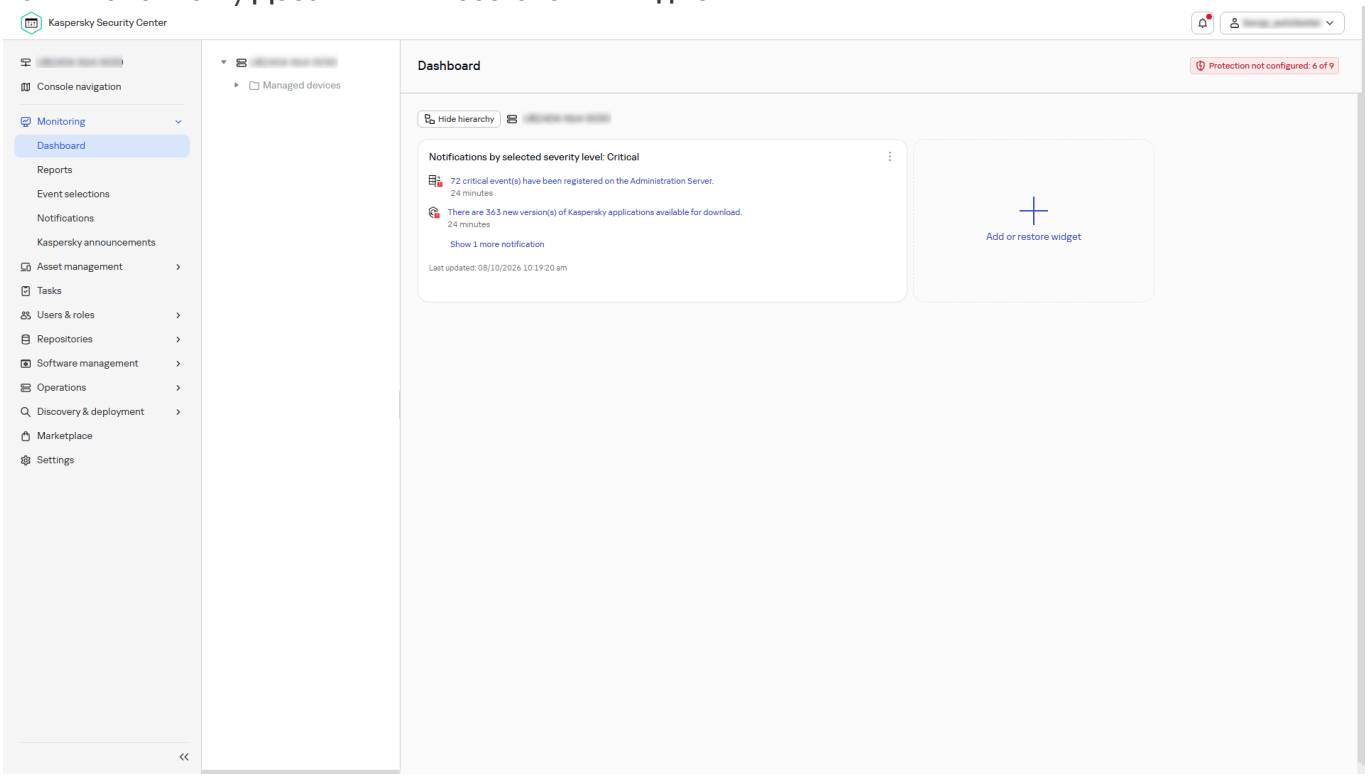
Чтобы добавить виджет на информационную панель:

1. В главном окне приложения перейдите в раздел **Мониторинг → Панель мониторинга**.



Панель мониторинга с виджетами

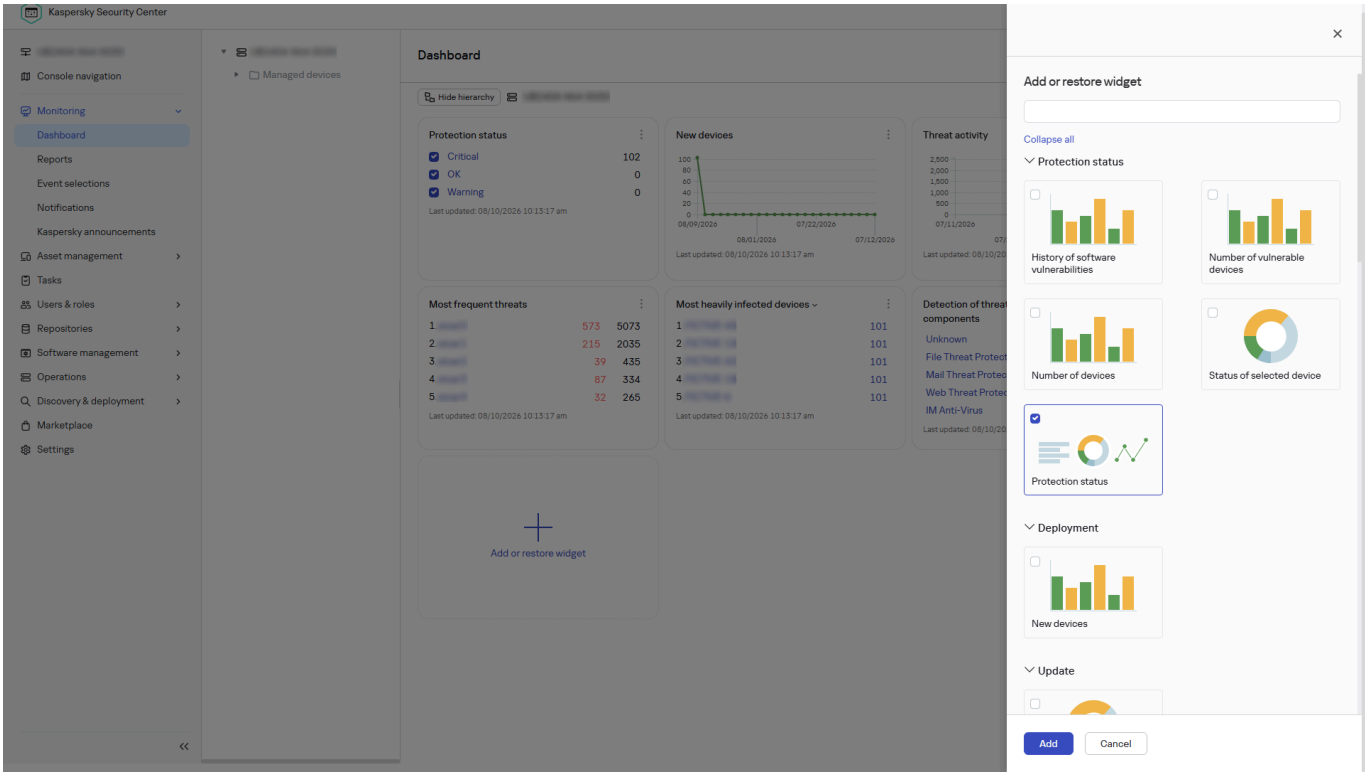
2. Нажмите на кнопку **Добавить или восстановить виджет**.



Добавление виджета

3. В списке доступных виджетов выберите виджет, который требуется добавить на информационную панель.

   Виджеты сгруппированы по категориям. Чтобы посмотреть, какие виджеты входят в категорию, нажмите на значок шеврона (>) рядом с именем категории.



Выбор типа виджета

4. Нажмите на кнопку **Добавить**.

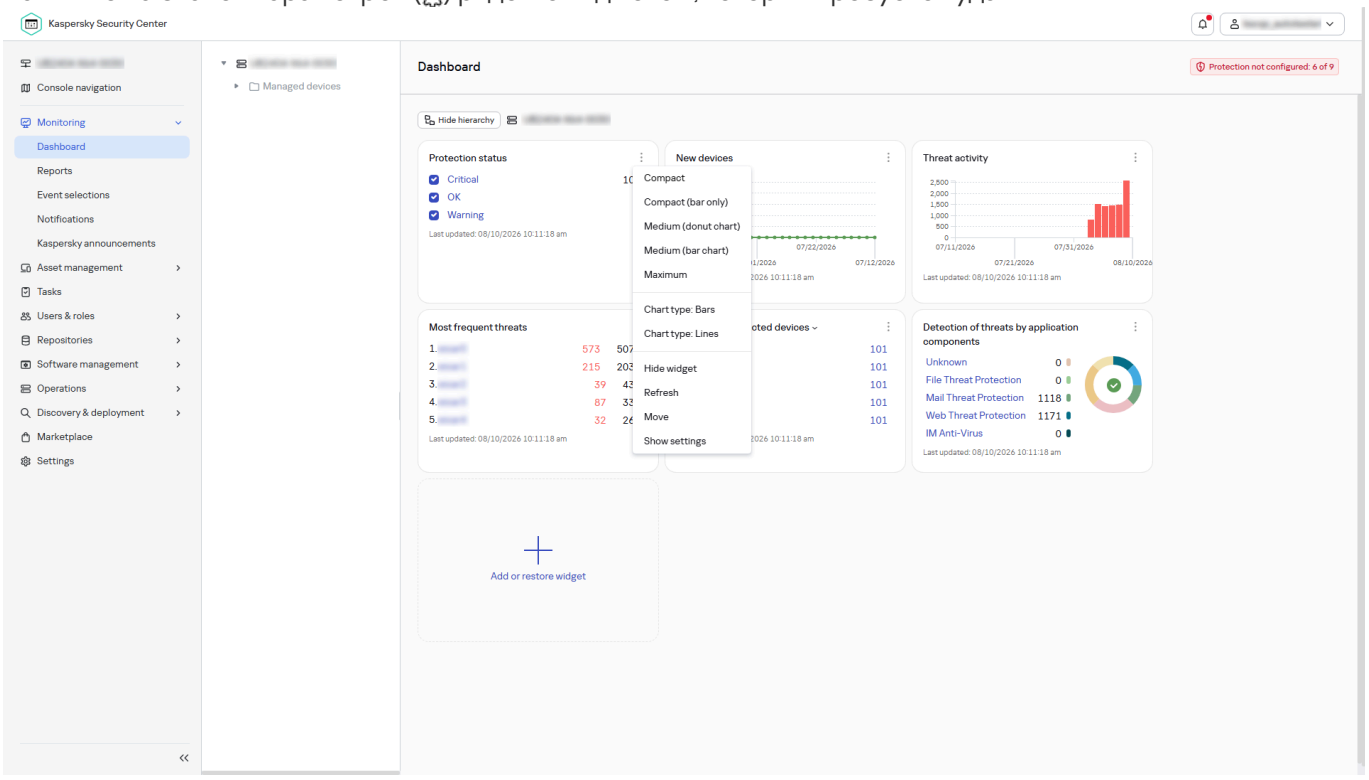
   Выбранные виджеты будут добавлены в конец информационной панели.

   Можно изменить внешний вид и параметры добавленных виджетов.

Удаление виджета с информационной панели

Чтобы удалить виджет с информационной панели:

1. В главном окне приложения перейдите в раздел **Мониторинг → Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с виджетом, который требуется удалить.



Меню виджета

3. Выберите **Скрыть виджет**.
4. В появившемся окне **Предупреждение** нажмите на кнопку **OK**.

Выбранный виджет будет удален с информационной панели. В дальнейшем можно опять добавить виджет на информационную панель.

Перемещение виджета на информационной панели

Чтобы переместить виджет на информационной панели:

1. В главном окне приложения перейдите в раздел **Мониторинг → Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с виджетом, который требуется переместить.
3. Выберите **Переместить**.
4. Укажите место, куда требуется переместить виджет. Можно выбрать только другой виджет.

Выбранные виджеты поменяются местами.

Изменение размера или внешнего вида виджета

Можно изменить внешний вид виджетов: выбрать столбчатую или линейную диаграмму. Для некоторых виджетов можно изменить размер: маленький, средний или крупный.

Чтобы изменить внешний вид виджета:

1. В главном окне приложения перейдите в раздел **Мониторинг → Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с виджетом, который требуется изменить.
3. Выполните одно из следующих действий:
   - Чтобы виджет отображался как столбчатая диаграмма, выберите **Тип диаграммы: линейчатая диаграмма**.
   - Чтобы виджет отображался как линейная диаграмма, выберите **Тип диаграммы: линейный график**.
   - Чтобы поменять размер области, занимаемой виджетом, выберите одно из значений:
     - **Минимальный**
     - **Минимальный (только линейчатая диаграмма)**
     - **Средний (кольцевой график)**
     - **Средний (линейчатая диаграмма)**
     - **Максимальный**

Внешний вид выбранного виджета будет изменен.

Изменение параметров виджета

Чтобы изменить параметры виджета:

1. В главном окне приложения перейдите в раздел **Мониторинг → Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с виджетом, который требуется изменить.
3. Выберите **Показать параметры**.
4. В открывшемся окне параметров виджета измените требуемые параметры виджета.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Параметры выбранного виджета будут изменены.

Набор параметров зависит от конкретного виджета. Ниже приведены некоторые общие параметры:

- **Область виджета** – набор объектов, для которых виджет отображает информацию; например, группа администрирования или выборка устройств.
- **Выберите задачу** – задача, для которой виджет отображает информацию.
- **Период** – период, за который отображается информация в 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 виджета вы можете обновить данные виджета вручную.

Чтобы обновить данные виджета:

1. В главном окне приложения перейдите в раздел **Мониторинг → Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с виджетом, который требуется переместить.
3. Нажмите на кнопку **Обновить**.

Данные 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 Linux (например, это может быть топ-менеджер). Когда у пользователя включен этот режим, у пользователя отображается только панель мониторинга с предопределенным набором виджетов. Таким образом, пользователь может просматривать указанную в 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 виджетами, например, добавлять или скрывать их. Поэтому нужно разместить в панели мониторинга все необходимые пользователю 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 **Изменение списков управления доступом объектов** в функциональной области **Общие функции: Права пользователя**. Если у вас нет этого права, вкладка для настройки режима будет отсутствовать.
- Пользователь с правом **Чтение** в области **Общие функции: Базовая функциональность**.

Если в вашей сети выстроена иерархия Серверов администрирования, для настройки режима Просмотра только панели мониторинга перейдите на тот Сервер, на котором учетная запись пользователя доступна на вкладке **Пользователи** в разделе **Пользователи и роли → Пользователи и группы**. Это может быть главный Сервер или физический подчиненный Сервер. На виртуальном Сервере администрирования настроить режим Просмотра только панели мониторинга невозможно.

Чтобы настроить режим Просмотра только панели мониторинга:

1. В главном окне приложения перейдите в раздел **Пользователи и роли → Пользователи и группы** и выберите вкладку **Пользователи**.
2. Нажмите на имя учетной записи пользователя, для которой вы хотите настроить панель инструментов с виджетами.
3. В открывшемся окне свойств учетной записи выберите вкладку **Панель мониторинга**.

   На открывшейся вкладке отображается та же панель мониторинга, что и для пользователя.
4. Если параметр **Отображать режим Просмотра только панели мониторинга** включен, выключите его переключателем.

   Когда этот параметр включен, также невозможно изменить панель мониторинга. После выключения параметра можно управлять виджетами.
5. Настройте внешний вид панели мониторинга. Набор виджетов, подготовленный на вкладке **Панель мониторинга**, доступен пользователю с настраиваемой учетной записью. Пользователь с такой учетной записью не может изменять какие-либо параметры или размер виджетов, добавлять или удалять виджеты с панели мониторинга. Поэтому настройте их под пользователя, чтобы он мог просматривать статистику защиты сети. Для этого на вкладке **Панель мониторинга** можно выполнять те же действия с виджетами, что и в разделе **Мониторинг → Панель мониторинга**:
   - Добавлять виджеты в панель мониторинга.
   - Скрывать виджеты, которые не нужны пользователю.
   - Перемещать виджеты в определенном порядке.
   - Изменять размер или внешний вид виджетов.
   - Изменять параметры 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 Linux, в том числе изменять параметры безопасности и виджеты.

7. Нажмите на кнопку **Сохранить**, когда закончите настройку режима Просмотра только панели мониторинга. Только после этого подготовленная панель мониторинга будет отображаться у пользователя.

8. Если пользователь хочет просмотреть статистику поддерживаемых приложений "Лаборатории Касперского" и ему нужны для этого права доступа, настройте права для этого пользователя. После этого данные приложений "Лаборатории Касперского" отображаются у пользователя в виджетах этих приложений.

Теперь пользователь может входить в Kaspersky Security Center Linux под настраиваемой учетной записью и просматривать статистику защиты сети в режиме Просмотра только панели мониторинга.

Отчеты администрирования и защиты

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 Web Console в разделе **Мониторинг → 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.

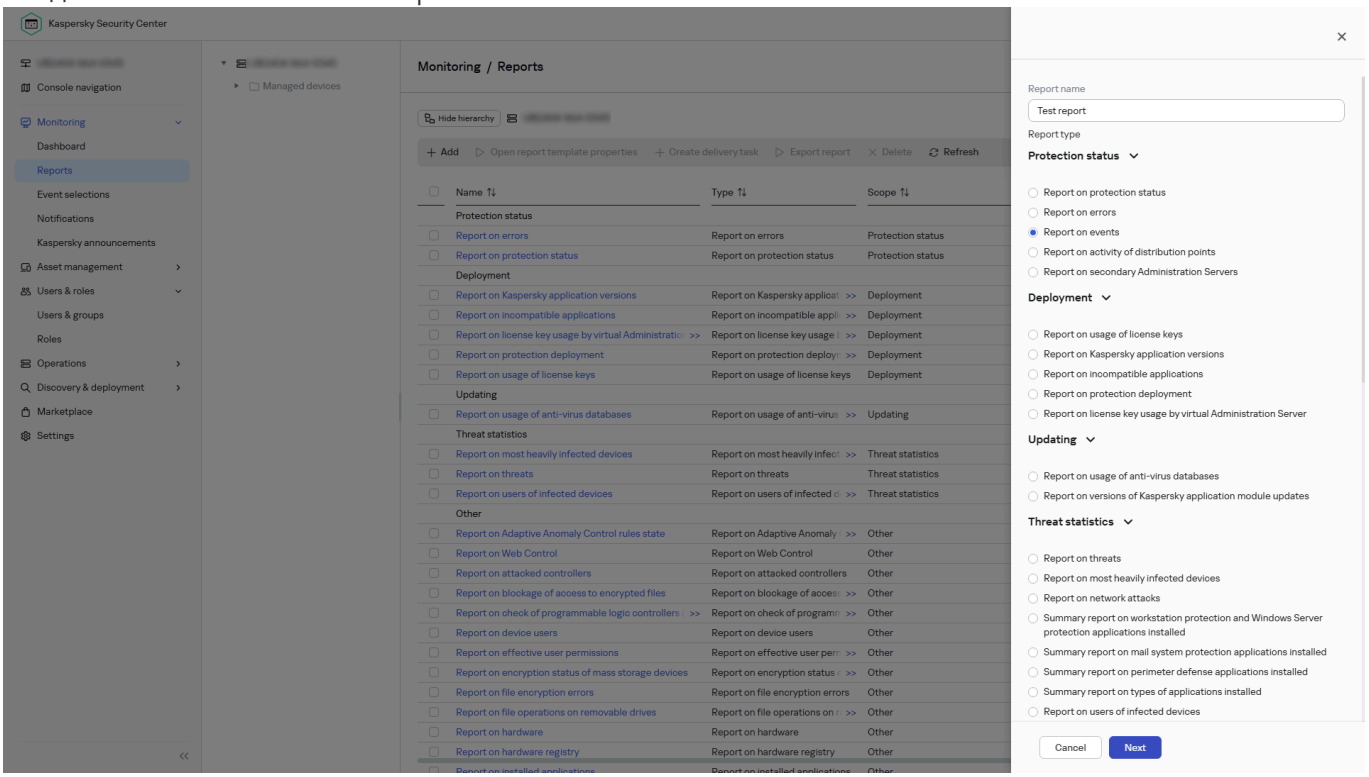
Можно создавать отчеты на основе существующих шаблонов, экспортировать отчеты в файл и создавать задачи рассылки отчетов.

Создание шаблона отчета

Чтобы создать шаблон отчета:

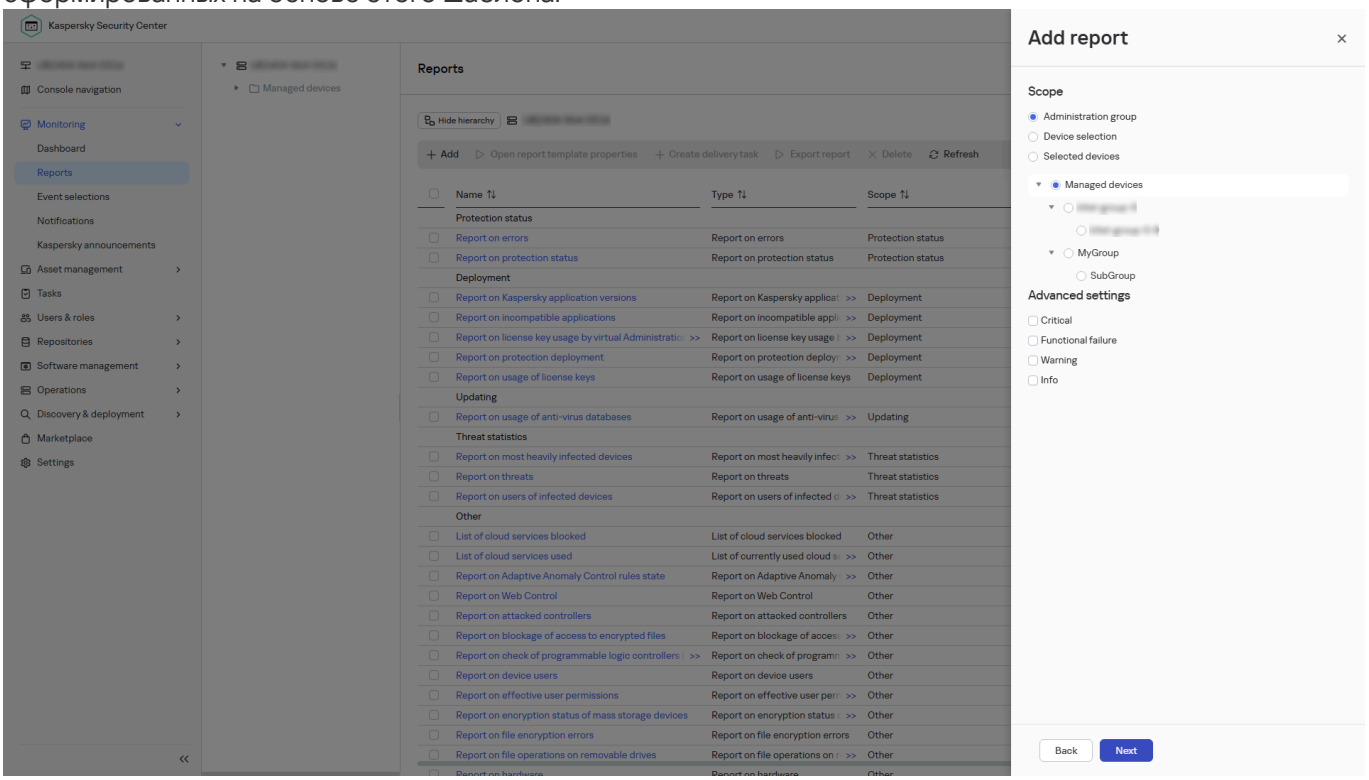
1. В главном окне приложения перейдите в раздел **Мониторинг** → **Отчеты**.
2. Нажмите на кнопку **Добавить**.

   В результате запустится мастер создания шаблона отчета. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Введите название отчета и выберите тип отчета.



Указание названия отчета и выбор типа 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.

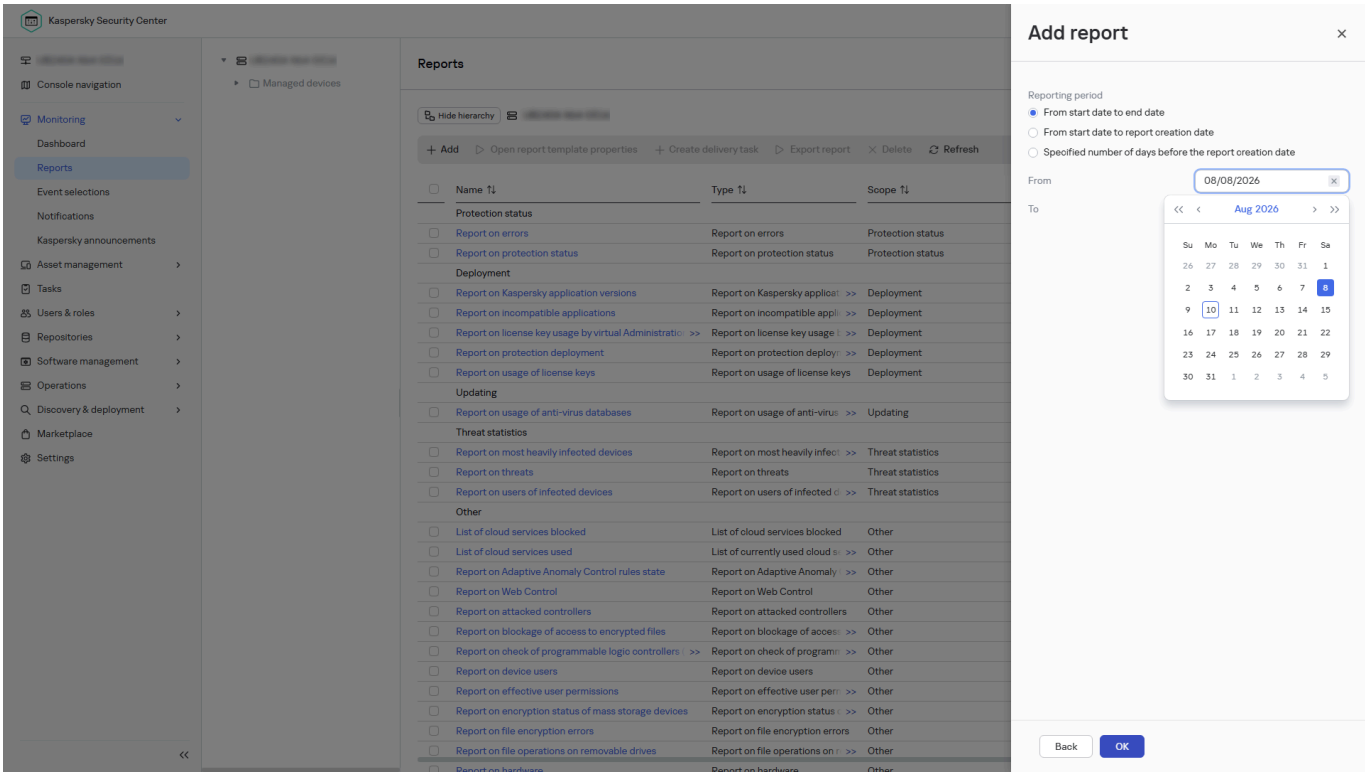


Выбор области действия отчета

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.



Выбор отчетного периода

6. Нажмите на кнопку **OK**, чтобы завершить работу мастера.

7. Выполните одно из следующих действий:

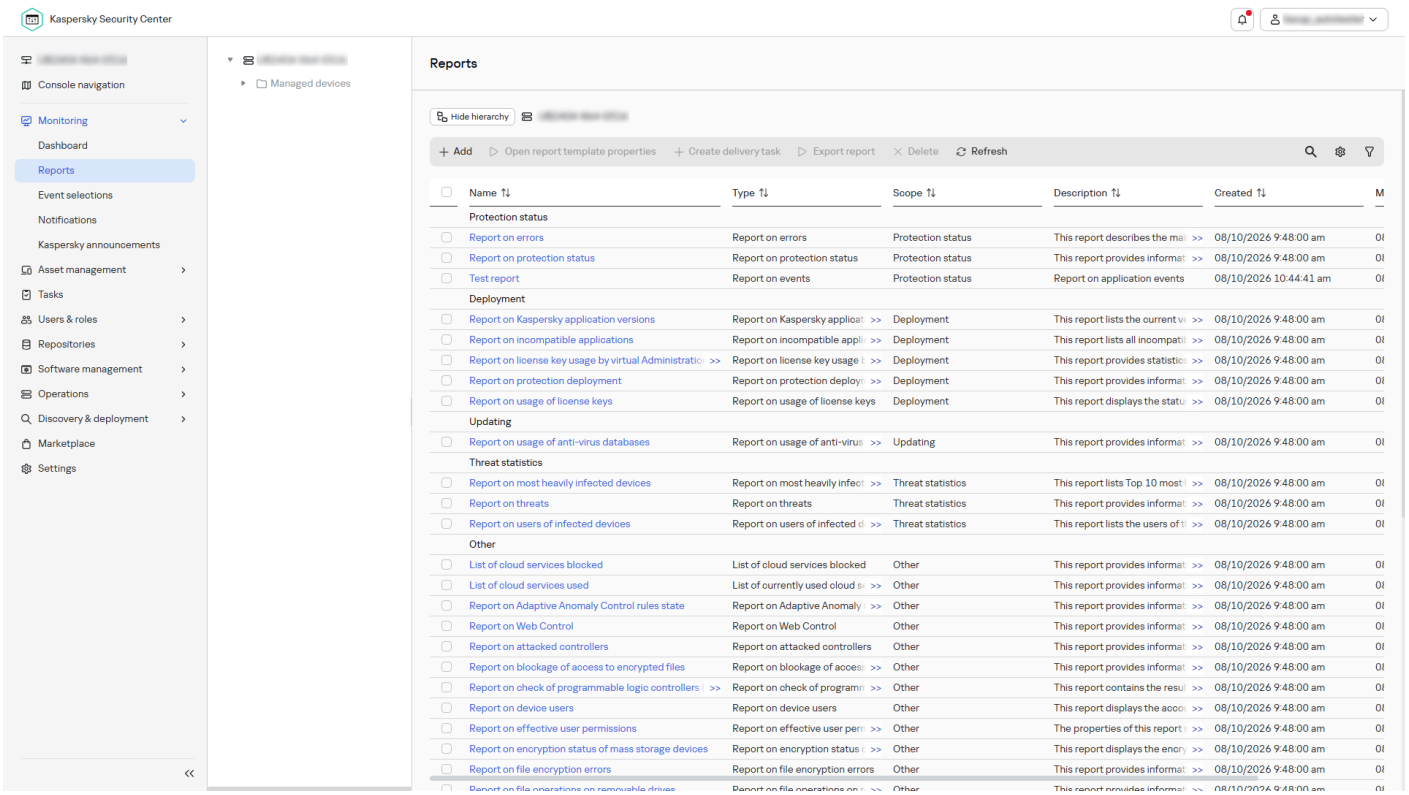
   - Нажмите на кнопку **Сохранить и запустить**, чтобы сохранить новый шаблон отчета и запустить формирование отчета на его основе.

     Шаблон отчета будет сохранен. Отчет будет сформирован.

   - Нажмите на кнопку **Сохранить**, чтобы сохранить новый шаблон отчета.

     Шаблон отчета будет сохранен.

Созданный шаблон можно использовать для формирования и просмотра отчетов.



Список отчетов

Просмотр и изменение свойств шаблона отчета

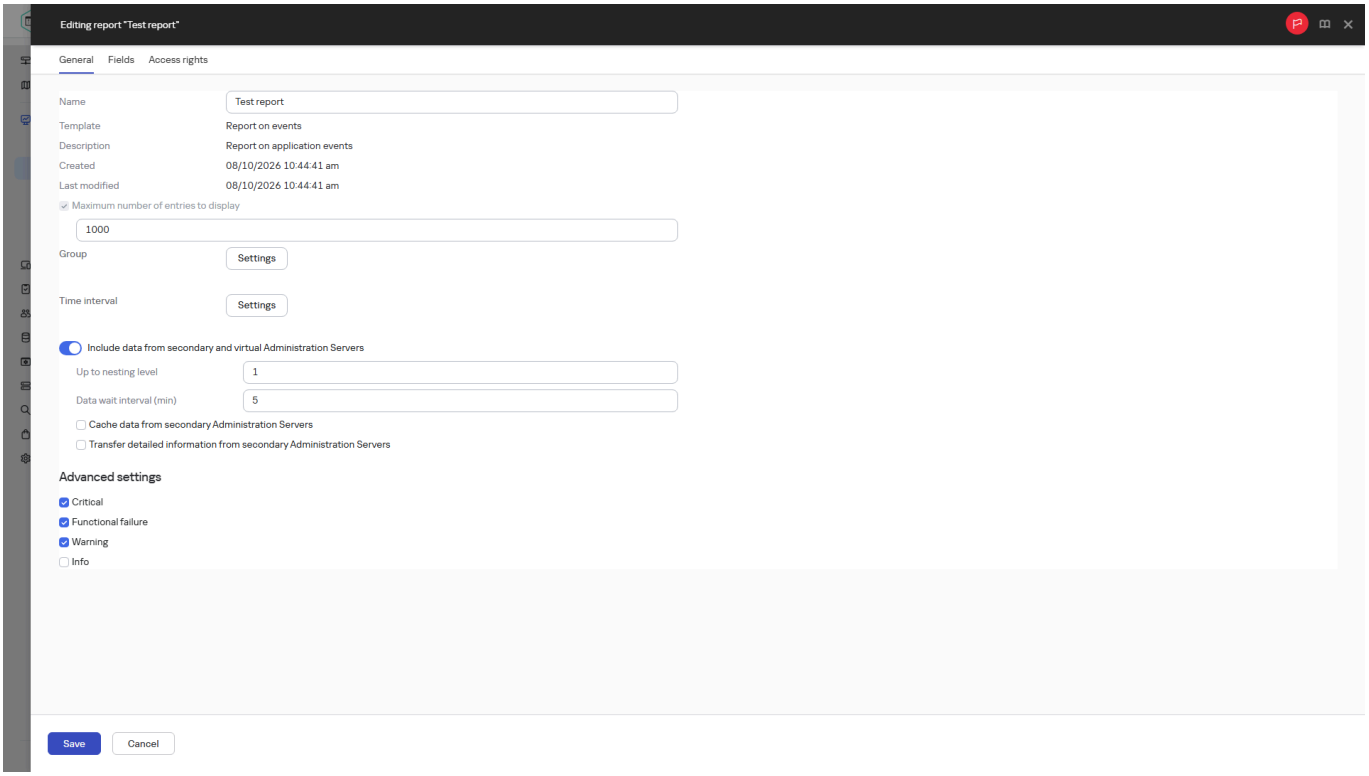
Вы можете просматривать и изменять основные свойства шаблона отчета, например, имя шаблона отчета или поля, отображаемые в отчете.

Чтобы просмотреть и изменить свойства шаблона отчета:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **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 вкладке **Общие**.



Свойства шаблона отчета

4. Измените свойства шаблона отчета:

- Вкладка **Общие**:
  - Название шаблона отчета
  - **Максимальное число отображаемых записей**

    Если этот параметр включен, количество отображаемых в таблице записей с подробными данными отчета не превышает указанное значение. Обратите внимание, что этот параметр не влияет на максимальное количество событий, которые вы можете включить в отчет при экспорте отчета в файл.

    Записи отчета сначала сортируются в соответствии с правилами, указанными в разделе **Поля** → **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 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 этого параметра позволяет просматривать информацию, полученную от подчиненных Серверов администрирования, даже если невозможно получить актуальные данные. Однако отображаемые данные могут быть устаревшими.

  По умолчанию параметр выключен.

- **Период обновления данных в кеше (ч)**

  Подчиненные Серверы администрирования 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.

- Вкладка **Поля**

  Выберите поля, которые будут отображаться в отчете. С помощью кнопок **Вверх** и **Вниз** измените порядок отображения полей. С помощью кнопок **Добавить** и **Изменить** укажите, будет ли информация в отчете фильтроваться или сортироваться по выбранным полям.

  В разделе **Фильтры детальных полей** вы также можете нажать на кнопку **Преобразовать фильтры**, чтобы начать использовать расширенный формат фильтрации. Этот формат позволяет комбинировать условия фильтрации, указанные в различных полях, с помощью логического ИЛИ. После нажатия на кнопку **Преобразовать фильтры**, справа открывается панель. Нажмите на кнопку **Преобразовать фильтры**, подтверждающую отзыв лицензии. Теперь вы можете определить преобразованный фильтр с условиями из раздела **Детальные данные**, которые применяются с помощью логического ИЛИ.

  > Преобразование отчета в формат, поддерживающий сложные условия фильтрации, сделает его несовместимым с предыдущими версиями Kaspersky Security Center (11 и ниже). Также в преобразованном отчете не будет данных с подчиненных Серверов администрирования с несовместимыми версиями.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

6. Закройте окно **Редактирование отчета <Название отчета>**.

Измененный шаблон отчета появится в списке шаблонов отчетов.

Экспорт отчета в файл

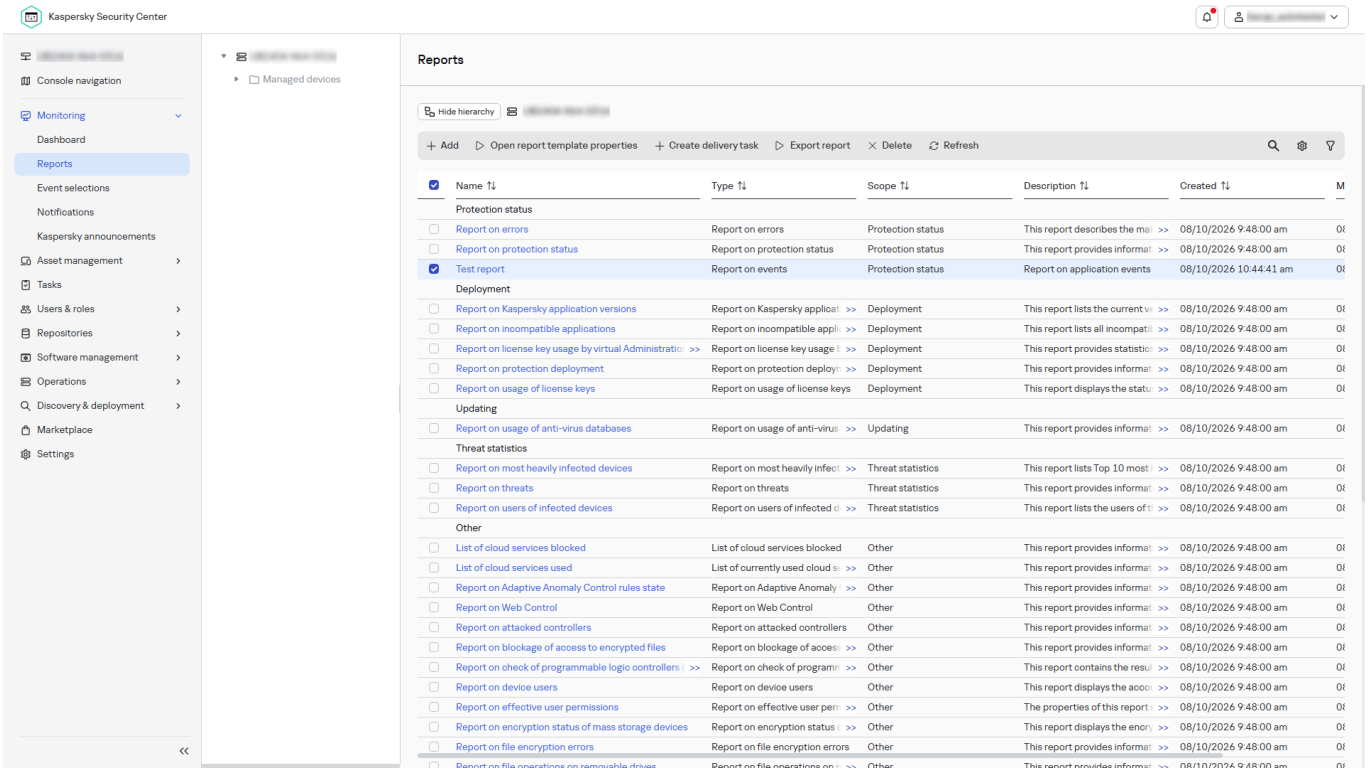
Вы можете сохранить один или несколько отчетов в форматах XML, HTML или PDF. Kaspersky Security Center Linux позволяет экспортировать до 10 отчетов в файлы указанного формата одновременно.

Чтобы экспортировать отчет в файл:

1. В главном окне приложения перейдите в раздел **Мониторинг → Отчеты**.

2. Выберите отчеты, которые вы хотите экспортировать.

Если вы выберете более десяти отчетов, кнопка **Экспортировать отчет** будет неактивна.



Список отчетов

3. Нажмите на кнопку **Экспортировать отчет**.

4. В открывшемся окне настройте следующие параметры экспорта:

   - **Имя файла**.

     Если вы выбрали один отчет для экспорта, укажите имя файла отчета.

     Если вы выбрали несколько отчетов, имена файлов отчетов будут совпадать с именами выбранных шаблонов отчетов.

   - **Максимальное количество записей**.

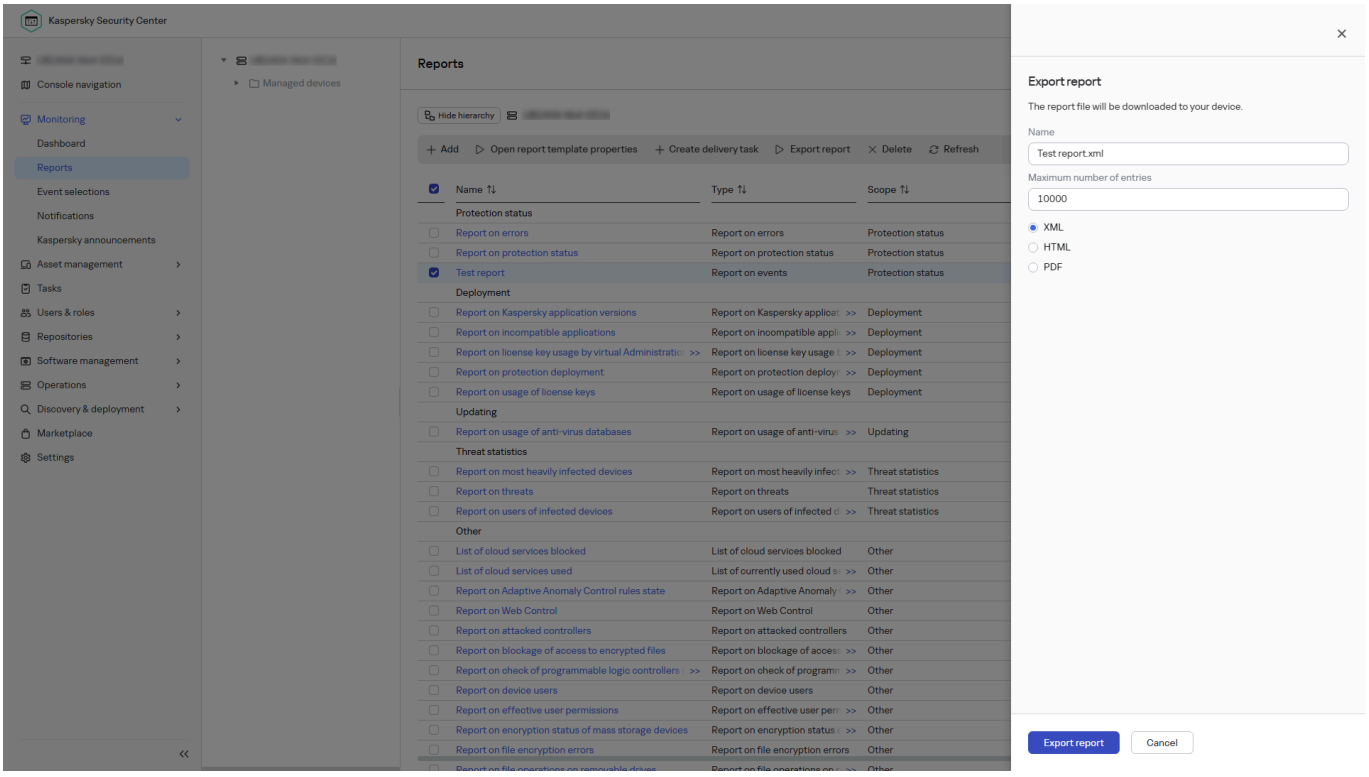
     Укажите максимальное количество записей, которые будут включены в файл отчета. По умолчанию указано значение 10 000.

     Вы можете экспортировать отчет с неограниченным количеством записей. Обратите внимание, что если ваш отчет содержит большое количество записей, время, необходимое для создания и экспорта отчета, увеличивается.

   - **Формат файла**.

     Выберите формат файла отчета: XML, HTML, или PDF. При экспорте нескольких отчетов все выбранные отчеты сохраняются в указанном формате в виде отдельных файлов.

Инструмент wkhtmltopdf необходим для преобразования отчета в формат PDF. При выборе параметра PDF Сервер администрирования проверяет, установлена ли на устройстве утилита wkhtmltopdf. Если инструмент не установлен, приложение выводит сообщение о том, что его необходимо установить на устройство с Сервером администрирования. Установите инструмент вручную, а затем переходите к следующему шагу.



Указание параметров экспорта отчета

5. Нажмите на кнопку **Экспортировать отчет**.

Отчет будет сохранен в файл в указанном формате.

Генерация и просмотр отчета

Чтобы сформировать и просмотреть отчет:

1. В главном окне приложения перейдите в раздел **Мониторинг → Отчеты**.

2. Нажмите на имя шаблона отчета, который вы хотите использовать для создания отчета.

   Отображается сгенерированный отчет с использованием выбранного шаблона.

Данные отчета отображаются в соответствии с языком локализации Сервера администрирования.

В сформированных отчетах некоторые шрифты могут некорректно отображаться на диаграммах. Чтобы избежать этого, установите библиотеку fontconfig. Также убедитесь, что в операционной системе установлены шрифты, соответствующие языковому стандарту вашей операционной системы.

В отчете отображаются следующие данные:

- На вкладке **Сводная информация**:
  - тип и название отчета, его краткое описание и отчетный период, а также информация о том, для какой группы устройств создан отчет;
  - графическая диаграмма с наиболее характерными данными отчета;
  - сводная таблица с вычисляемыми показателями отчета.
- На вкладке **Подробнее** отобразится таблица с подробными данными отчета.

Создание задачи рассылки отчета

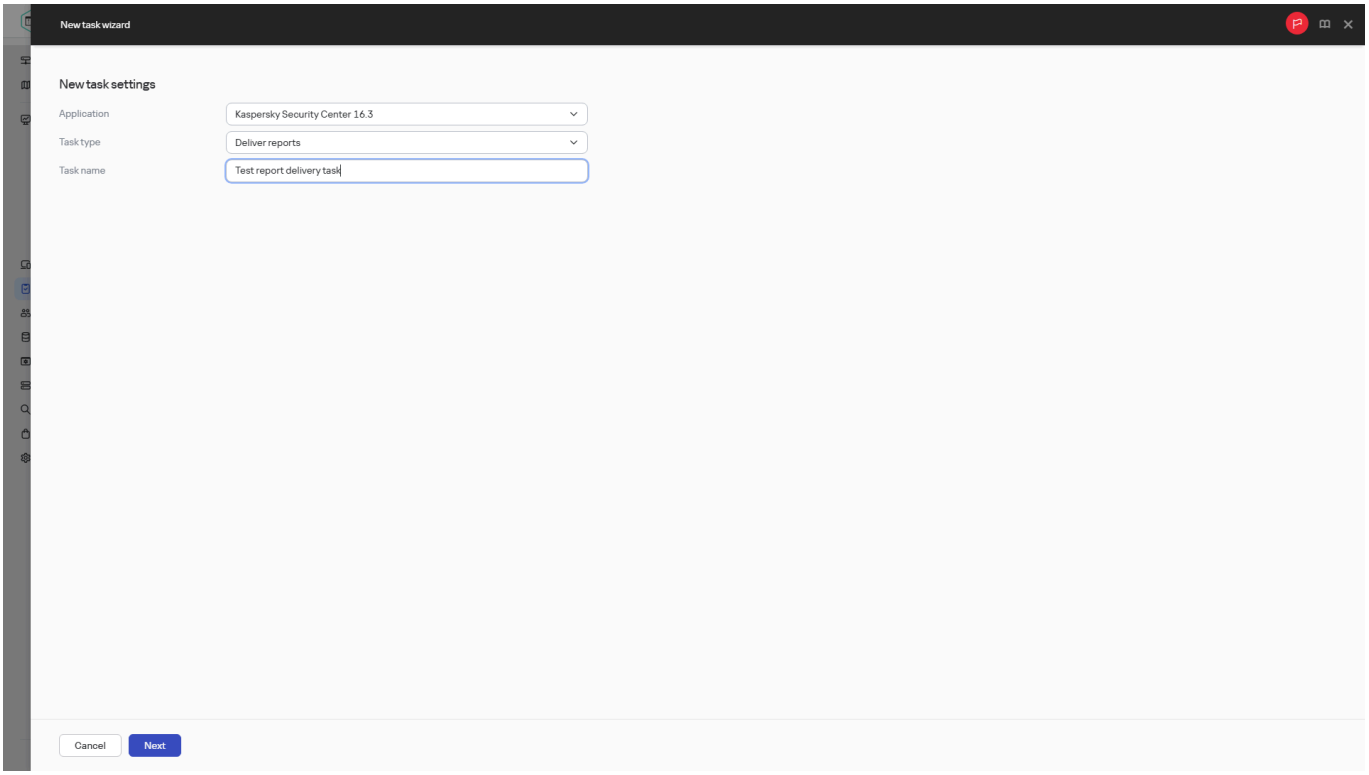
Можно создать задачу рассылки выбранных отчетов.

Чтобы создать задачу рассылки отчета:

1. В главном окне приложения перейдите в раздел **Мониторинг → Отчеты**.
2. Установите флажки рядом с шаблонами отчетов, на основе которых вы хотите сформировать задачу рассылки отчетов.
3. Нажмите на кнопку **Создать задачу рассылки отчетов**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
4. На шаге мастера **Параметры новой задачи** введите название задачи.

   Название задачи по умолчанию – **Рассылка отчетов.** Если задача с таким названием уже существует, к названию задачи добавляется порядковый номер (<N>).



Создание задачи рассылки отчета

5. На шаге мастера **Конфигурация отчета** укажите следующие параметры:

   a. Шаблоны отчетов, рассылаемых задачей.

   b. Формат отчета: HTML, XLS или PDF.

      Инструмент wkhtmltopdf необходим для преобразования отчета в формат PDF. При выборе параметра PDF Сервер администрирования проверяет, установлена ли на устройстве утилита wkhtmltopdf. Если инструмент не установлен, приложение выводит сообщение о том, что его необходимо установить на устройство с Сервером администрирования. Установите инструмент вручную, а затем переходите к следующему шагу.

   c. Будут ли отчеты рассылаться по электронной почте, а также параметры почтовых уведомлений.

      Вы можете указать до 20 адресов электронной почты. Чтобы разделить адреса электронной почты, нажмите на клавишу **Enter**. Вы также можете вставить список адресов электронной почты, разделенных запятыми, и нажать на клавишу **Enter**.

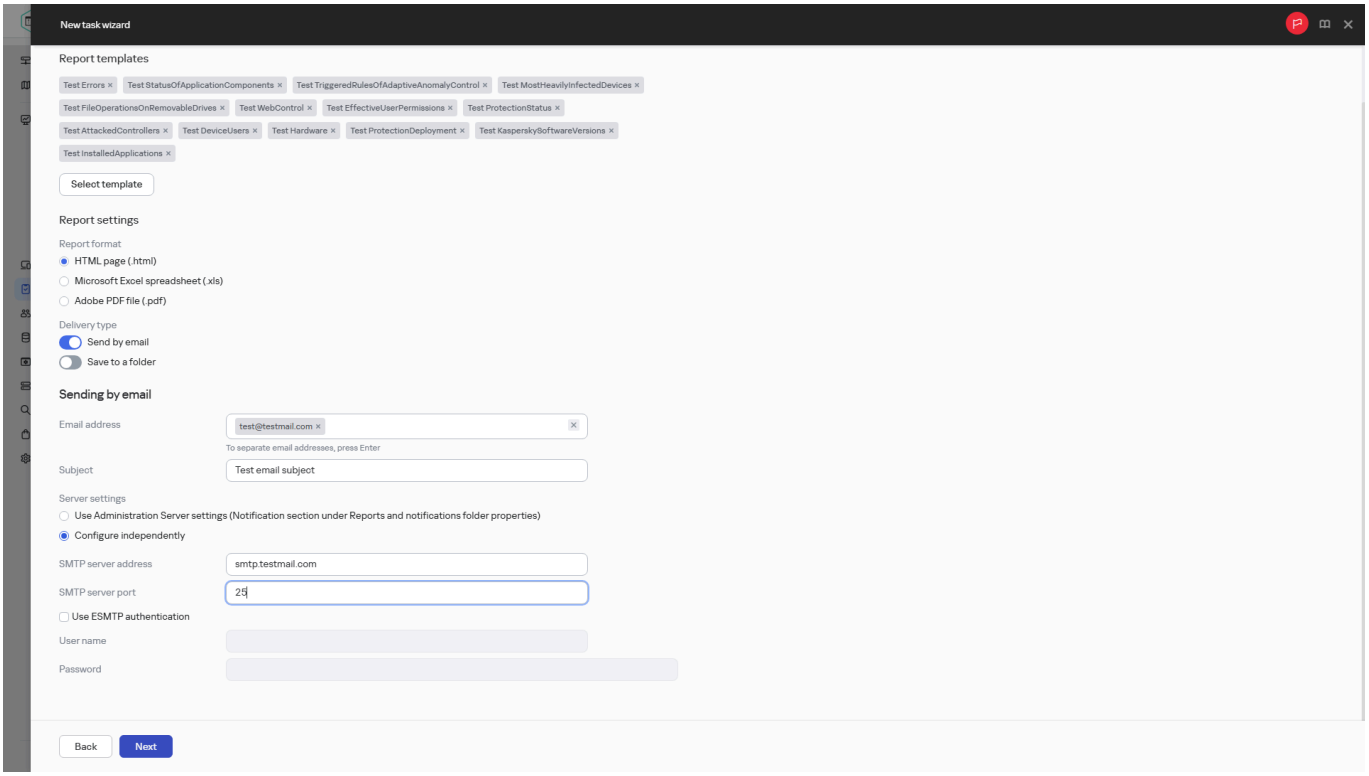
   d. Будут ли отчеты сохраняться в папку вместе с соответствующими параметрами.

      После того как вы включите параметр **Сохранить 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.



Указание параметров задачи

6. На шаге мастера **Настройка расписания запуска задачи** выберите расписание запуска задачи.

   Доступны следующие варианты расписания запуска задачи:

   - **Вручную**

     Задача не запускается автоматически. Вы можете запустить задачу только вручную.

     По умолчанию выбран этот вариант.

   - **Каждые N минут**

     Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

     По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

   - **Каждый N час**

     Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

     По умолчанию задача запускается каждые 6 часов, начиная с текущих системной даты и времени.

   - **Каждые N дней**

     Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются приложением, для которого вы создаете задачу.

     По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

  По умолчанию задача запускается каждую пятницу в текущее системное время.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **В указанные дни**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию указано время 18:00 и не выбраны дни месяца.

  > Обратите внимание, что вы выбираете порядковый номер дня недели в месяце, а не конкретную дату в месяце или номер недели (первая, вторая неделя месяца). Например, если вы выберите ячейку **Вт** в строке **Первая**, в этом случае задача будет запускаться каждый первый вторник каждого нового месяца.

  Вы можете выбрать несколько дней недели.

- **При обнаружении вирусной атаки**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы приложений, которые будут отслеживать вирусные атаки. Доступны следующие типы приложений:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы приложений.

  Вы можете запускать разные задачи в зависимости от типа приложения безопасности, сообщающего о вирусной атаке. В этом случае удалите выбор типов приложений, которые вам не нужны.

- **По завершении другой задачи**

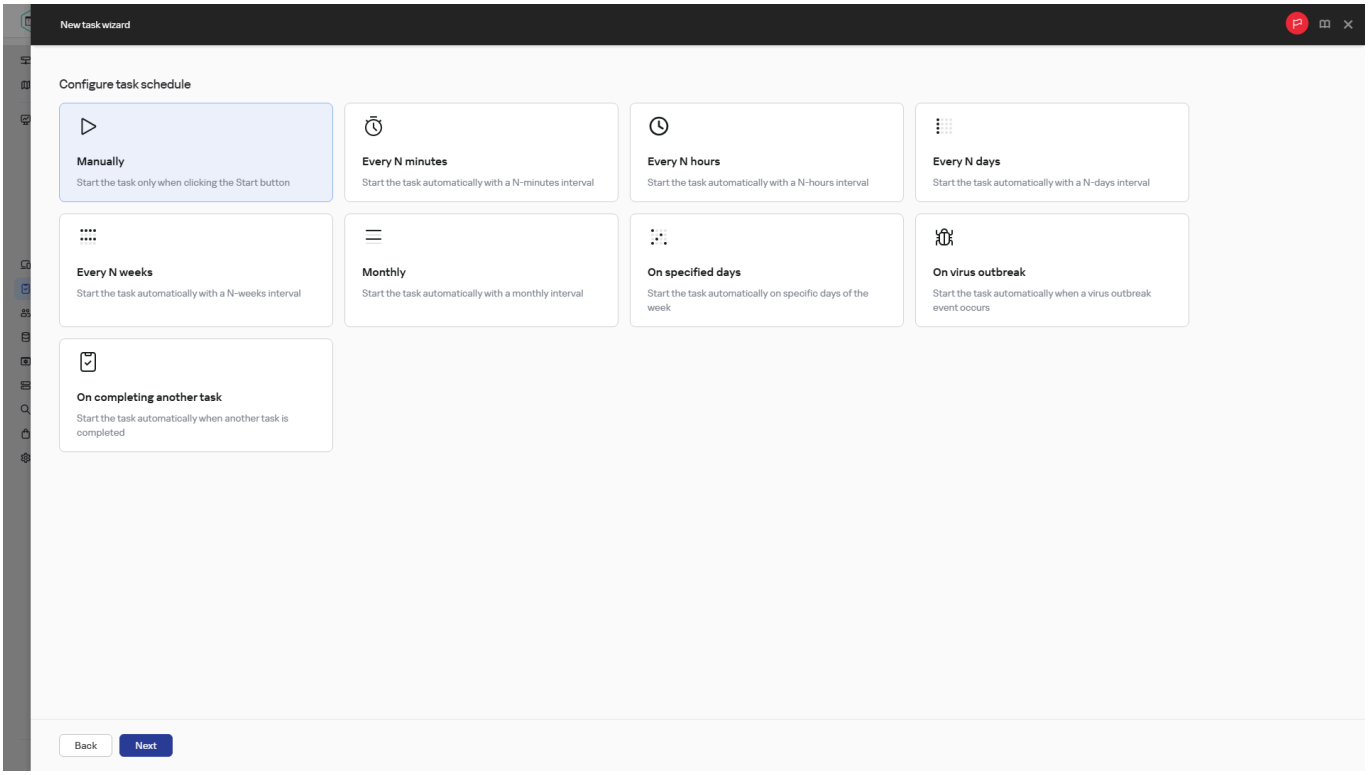
  Текущая задача будет запущена после завершения другой задачи. Этот параметр работает, только если обе задачи назначены одним и тем же устройствам. Например, вы можете запустить задачу *Управление устройствами* с помощью параметра **Включить устройство** и после ее завершения запустить задачу *Поиск вирусов*, как запускающую задачу.

  Вам нужно выбрать запускающую задачу из таблицы и статус, с которым эта задача должна завершиться (**Завершена успешно** или **Сбой**).

При необходимости вы можете искать, сортировать и фильтровать задачи в таблице следующим образом:

- Введите название задачи в поле поиска, чтобы выполнить поиск задачи по названию.
- Нажмите на значок сортировки, чтобы отсортировать задачи по имени.

  По умолчанию задачи отсортированы в алфавитном порядке по возрастанию.
- Нажмите на значок фильтра и в открывшемся окне отфильтруйте задачи по группам, после чего нажмите на кнопку **Применить**.



Выбор расписания запуска задачи

7. На этом шаге мастера настройте другие параметры расписания запуска задачи:

- В разделе **Расписание задачи** проверьте или перенастройте ранее выбранное расписание и установите период, дни месяца или недели, задайте условие вирусной атаки или выполнение другой задачи в качестве запуска задачи. В этом разделе также можно указать время запуска, если выбрано подходящее расписание.
- В разделе **Дополнительные параметры** укажите следующие параметры:
  - **Запускать пропущенные задачи**

    Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

    Если параметр включен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

    Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию. Для расписания **Вручную**, **Один раз** и **Немедленно** задачи выполняются только на тех клиентских устройствах, которые видны в сети. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

По умолчанию параметр включен.

- **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.

  По умолчанию параметр включен.

- **Использовать автоматическую случайную задержку запуска задачи в интервале**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

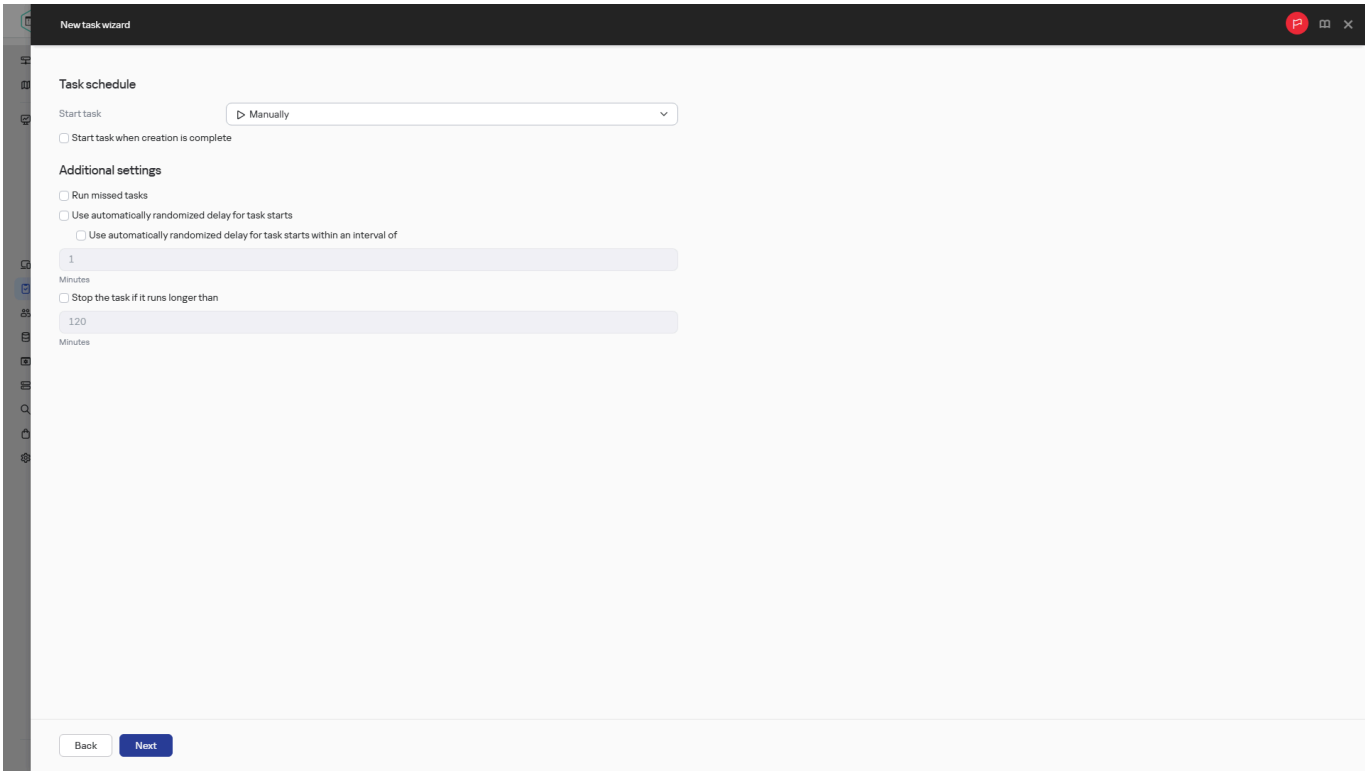
  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

- **Остановить, если задача выполняется дольше**

  По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

  Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

  По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

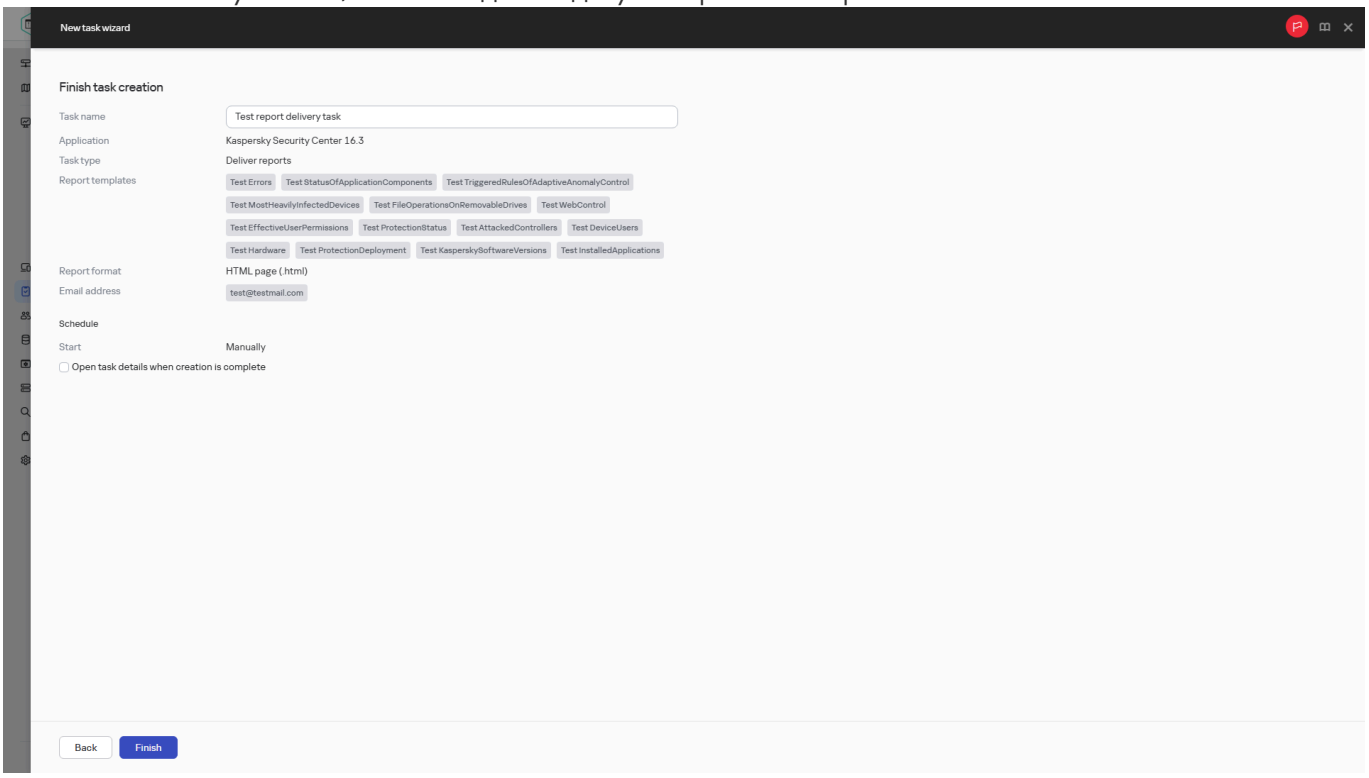


Указание параметров запуска задачи

8. На шаге мастера **Выбор учетной записи для запуска задачи** укажите учетные данные учетной записи, которая используется для запуска задачи.

9. Если требуется изменить другие параметры задачи после ее создания, на шаге мастера **Завершение создания задачи** включите параметр **Открыть окно свойств задачи после ее создания**. По умолчанию параметр включен.

10. Нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.



Завершение создания задачи

Будет создана задача отправки отчета. Если параметр **Открыть окно свойств задачи после ее создания** включен, откроется окно параметров задачи.

Удаление шаблонов отчетов

Чтобы удалить шаблоны отчетов:

1. В главном окне приложения перейдите в раздел **Мониторинг → Отчеты**.

2. Установите флажки напротив шаблонов отчетов, которые требуется удалить.

3. Нажмите на кнопку **Удалить**.

4. В появившемся окне нажмите на кнопку **OK**, 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.

Центр усиления безопасности

В Центре усиления безопасности отображается актуальная информация о защите Сервера администрирования и точек распространения. Информация представлена в виде индикаторов уровня защиты. Индикаторы позволяют отслеживать внедрение Руководства по усилению защиты, а также вовремя решать проблемы безопасности вашей инфраструктуры при их возникновении.

Индикатор может находиться в одном из следующих статусов:

- Защита настроена.
- Защита настроена частично.
- Защита не настроена.

Как просмотреть подробную информацию об уровне защиты

Общий статус индикатора формируется в зависимости от состояния параметров защиты.

*Чтобы открыть **Центр усиления защиты**:*

1. В главном меню перейдите в раздел **Мониторинг** → **Панель мониторинга**.
2. В правом верхнем углу нажмите на статус защиты.

   В открывшемся окне **Центр усиления защиты** параметры будут сгруппированы по защищаемым объектам: Сервер администрирования и точки распространения.

Каждый параметр защиты отображается в одном из состояний в зависимости от ваших прав доступа:

- ✅ – если нет проблем, которые нужно решить, или у вас нет необходимых прав доступа.
- ⚠️ или ❌ – если есть проблемы, требующие решения.

Следующие параметры отображаются только для Сервера администрирования:

- Резервное копирование настроено.
- Обслуживание Сервера администрирования настроено.
- Шифрование TLS включено.

Следующие параметры отображаются и для Сервера администрирования и для точек распространения:

- Приложение безопасности установлено.
- Политика приложения безопасности применена.
- Обновление антивирусных баз настроено.

- Все устройства управляемые.

  Также этот параметр отображается для устройств, не являющихся точками распространения или устройствами с Сервером администрирования.

Особенности для Сервера администрирования:

- Все параметры защиты рассчитываются только для физического Сервера администрирования и не применяются к виртуальным Серверам.

  Если у вас есть иерархическая структура из нескольких Серверов администрирования, показатель уровня защиты рассчитывается для каждого физического Сервера отдельно.

- Параметры **Приложение безопасности установлено**, **Политика приложения безопасности применена** и **Обновление антивирусных баз настроено** рассчитываются для устройства с установленным Сервером администрирования.

- При развертывании отказоустойчивого кластера Kaspersky Security Center Linux для каждого узла рассчитываются параметры **Приложение безопасности установлено**, **Политика приложения безопасности применена, Обновление антивирусных баз настроено** и **Все устройства управляемые**. Узел учитывается при расчете статуса индикатора только после того, как станет активным.

Как рассчитывается статус индикатора

В таблице ниже описано, как рассчитывается статус индикатора.

Состояние индикатора	Условие
Защита настроена.	Все параметры защиты указаны в статусе .
Защита настроена частично.	Параметр **Обновление антивирусных баз настроено** находится в статусе , а все остальные параметры находятся в статусе .
Защита не настроена.	Если хотя бы один из следующих параметров защиты находится в статусе .

Установлено приложение безопасности

Приложения безопасности позволяют защитить ваши устройства от различных типов угроз, включая сетевые, фишинговые и мошеннические атаки.

Параметр отображается в статусе , если выполняется ли одно из условий:

- У вас нет прав доступа к устройствам.
- У вас есть право **Чтение** в функциональной области **Общие функции → Базовая функциональность**, при этом на устройствах установлены Агент администрирования и приложение безопасности.

  Условие должно выполняться на всех устройствах, доступных вам в соответствии с вашими правами доступа, за исключением: устройств с установленным приложением, которое не требует антивирусной защиты (например, защищенная операционная система), устройств без установленного Агента администрирования, информация о которых появилась на Сервере администрирования менее чем 24 часа назад, автономных устройств, которые в последний раз подключались к Серверу администрирования семь дней назад или более.

Параметр отображается в статусе , если выполняется хотя бы одно из условий ниже.

Нажмите на кнопку **Просмотреть устройства** и выполните действия, описанные в таблице, для устройств которые отобразятся.

Условие	Решение
Агент администрирования не установлен на устройстве	Установить Агент администрирования. Для устройства с Сервером администрирования самый простой способ установки Агента администрирования – использовать автономный инсталляционный пакет.
Устройство включено в группу **Нераспределенные устройства**	Переместите устройство в группу Управляемые устройства или в ее подгруппу.
Приложения безопасности не найдены или для установленного приложения безопасности постоянная защита не работает	Установите приложение безопасности. Приложение передает данные о состоянии защиты на Сервер администрирования. Вы можете просмотреть состояние защиты устройства в свойствах устройства: раздел **Общие → Статус устройства**. На устройстве Сервера администрирования нужно установить Kaspersky Endpoint Security для Linux.

Политика применена

Политика – это набор параметров приложения безопасности, которые применяются к группе администрирования и ее подгруппе.

Параметр отображается в статусе , если выполняется ли одно из условий:

- У вас нет прав доступа к устройствам.
- У вас есть право **Чтение** в функциональной области **Общие функции → Базовая функциональность**, приложение безопасности установлено на ваших устройствах, и к устройствам применяется активная политика этого приложения безопасности.

> Условие должно выполняться на всех устройствах, доступных вам в соответствии с вашими правами доступа, за исключением: устройств с установленным приложением, которое не требует антивирусной защиты (например, защищенная операционная система), устройств без установленного Агента администрирования, информация о которых появилась на Сервере администрирования менее чем 24 часа назад, автономных устройств, которые в последний раз подключались к Серверу администрирования семь дней назад или более.

Параметр отображается в статусе , если выполняется хотя бы одно из условий ниже.

Нажмите на кнопку **Просмотреть устройства** и выполните действия, описанные в таблице, для устройств которые отобразятся.

Условие	Решение
Приложение безопасности не установлено на устройстве.	Убедитесь, что устройство отсутствует в выборке для параметра защиты **Установленное приложение безопасности**.
К устройству не применяется политика.	Убедитесь, что для группы администрирования к которой принадлежит устройство, создана политика. Если нет, создайте активную политику. Если да, убедитесь, что: • Созданная политика активна. Если нет, активируйте политику. • Статус распространения политики: **Применена успешно**. Если статус **Применено с ошибкой**, проблема должна быть устранена на стороне приложения безопасности.

Обновление антивирусных баз настроено

Поскольку антивирусные базы защищают ваши устройства от угроз, вам нужно регулярно и своевременно выполнять обновление баз на устройствах.

Параметр отображается в статусе , если выполняется ли одно из условий:

- У вас нет прав доступа к устройствам.
- У вас есть право Чтение в функциональной области Общие функции → Базовая функциональность и антивирусные базы обновлены на устройствах.

> Условие должно выполняться на всех устройствах, доступных вам в соответствии с вашими правами доступа, за исключением: устройств с установленным приложением, которое не требует антивирусной защиты (например, защищенная операционная система), устройств без установленного Агента администрирования, информация о которых появилась на Сервере администрирования менее чем 24 часа назад, автономных устройств, которые в последний раз подключались к Серверу администрирования семь дней назад или более.

Параметр отображается в статусе ⚠, если антивирусные базы обновлялись на устройстве более 3 дней назад.

Параметр отображается в статусе ✖, если антивирусные базы обновлялись на устройстве более 7 дней назад.

Чтобы решить проблему:

1. Нажмите на кнопку Просмотреть устройства рядом с параметром.
2. Для отображаемых устройств выполните следующие действия:
   a. Убедитесь, что между Агентом администрирования и Сервером администрирования установлено соединение.

      Если нет, см. следующие статьи:

      Устранение проблем с обновлением антивирусных баз Kaspersky Endpoint Security для Linux

      Проблемы при обновлении антивирусных баз из хранилища Kaspersky Security Center

   b. Убедитесь, что работа приложения "Лаборатории Касперского", антивирусные базы которого вы используете, не останавливается.

      Если приложение остановлено, запустите его.

   c. На устройстве просмотрите ошибки, возникшие после обновления.

Резервное копирование настроено

Рекомендации по резервному копированию данных Сервера администрирования см. в разделе Резервное копирование и восстановление данных Сервера администрирования.

Параметр отображается в статусе ✔, если выполняется ли одно из условий:

- У вас нет прав для работы с задачей резервного копирования данных Сервера администрирования.
- У вас есть права **Чтение, Запись** и **Выполнение** в функциональной области **Общие функции → Операции с Сервером администрирования** и настроено регулярное выполнение задачи резервного копирования данных.

Параметр отображается в статусе ✖, если выполняется хотя бы одно из условий ниже.

Условие	Решение
Задача резервного копирования данных Сервера администрирования не создана.	Создайте задачу.
Не настроены необходимые параметры расписания запуска задачи резервного копирования данных Сервера администрирования.	В задаче обслуживания Сервера администрирования укажите параметры **Запуск задачи**, отличные значений **При обнаружении вирусной атаки** и **Вручную**.

Обслуживание Сервера администрирования настроено

Обслуживание Сервера администрирования позволяет освободить место в папке Сервера администрирования, а также минимизировать размер базы данных. Это помогает ускорить обработку запросов и повышает общую стабильность системы.

Параметр отображается в статусе ✅, если выполняется ли одно из условий:

- У вас нет прав для работы с задачей обслуживания Сервера администрирования.
- У вас есть права **Чтение, Запись** и **Выполнение** в функциональной области **Общие функции → Операции с Сервером администрирования** и настроено регулярное выполнение задачи обслуживания Сервера администрирования.

  > Права должны быть установлены на уровне Сервера администрирования.

Параметр отображается в статусе ❌, если выполняется хотя бы одно из условий ниже.

Условие	Решение
Задача обслуживания Сервера администрирования не создана.	Создайте задачу.
Не настроены необходимые параметры расписания запуска задачи обслуживания Сервера администрирования.	В задаче обслуживания Сервера администрирования укажите параметры **Запуск задачи**, отличные значений **При обнаружении вирусной атаки** и **Вручную**.

Шифрование TLS включено

Вам нужно убедиться, что для протокола TLS разрешены только версии 1.2 и 1.3. Разрешение более ранних версий приведет к серьезным рискам безопасности данных и сделает системы уязвимыми для атак.

Параметр отображается в статусе ✅, если для протокола TLS разрешены только версии 1.2 и 1.3.

Параметр отображается в статусе ❌, если для протокола TLS разрешены версии ниже 1.2.

Чтобы решить проблему, вам нужно для флага `SrvUseStrictSslSettings` установить значение `4` или `5`.

Все устройства управляемые

С помощью параметра вы можете выявить устройства, над которыми потенциально потеряно управление.

Чтобы Сервер администрирования мог обнаружить управляемое устройство при сканировании сети, вам нужно настроить регулярный опрос IP-диапазонов или опрос сети Windows. При этом периодичность опроса следует установить не более, чем три суммарных периода синхронизации Агента администрирования с учетом времени на обработку данных опроса.

Устройства, которым назначен меньший период синхронизации, могут ошибочно влиять на состояние индикатора.

Расчеты интервалов опроса для выбранных периодов синхронизации представлены в таблице.

Период синхронизациив (мин)	Количество управляемых устройств	Максимальные интервалы опроса IP и сети Windows (мин)
15	10 000	35
30	20 000	80
45	30 000	120
60	40 000	165
75	50 000	210

Пересчет статуса параметра может занять некоторое время.

Параметр отображается в статусе ✅ при выполнении одного из условий:

- У вас нет прав доступа к устройствам.
- У вас есть право **Чтение** в функциональной области **Общие функции** → **Базовая функциональность**, при этом устройства находятся в группе **Управляемые устройства** и установлено соединение между Сервером администрирования и Агентом администрирования на устройствах.

  Условие должно выполняться на всех устройствах, доступных вам в соответствии с вашими правами доступа, за исключением: устройств, информация о которых появилась на Сервере администрирования менее 24 часов назад, и устройств, которые в последний раз подключались к Серверу администрирования семь дней назад или более.

Параметр отображается в статусе ❌ при наличии хотя бы одного устройства, для которого выполняется одно из условий ниже.

Нажмите на кнопку **Просмотреть устройства** и выполните действия, описанные в таблице, для устройств, которые отобразятся.

Условие	Решение
На устройстве, входящем в группу **Управляемые устройства**, не установлен Агент администрирования.	Установить Агент администрирования.

Сервер администрирования обнаруживает управляемое устройство при сканировании сети, но соединение этого устройства с Сервером администрирования не было установлено в течение трех периодов синхронизации.	Выполните следующие действия: 1. Запустите утилиту klnagchk на проблемном устройстве, чтобы проверить работу службы и подключение Агента администрирования к Серверу администрирования. 2. Проверьте сетевую доступность Сервера администрирования и шлюзов соединений. 3. Восстановите подключение устройства к Серверу администрирования с помощью утилиты klmover. 4. Удалите устаревшие устройства из групп администрирования. Если в вашей инфраструктуре есть управляемые устройства, которые в выключенном состоянии продолжают отвечать на опросы сети, такие устройства могут ошибочно влиять на состояние индикатора. Вы можете выполнить следующие действия для проблемных устройств: a. Убедиться, что устройство управляется Сервером администрирования. b. Переместить это устройство в отдельную группу администрирования. c. В этой группе администрирования присвоить условию **Устройство стало неуправляемым** любой статус, кроме *Критический*.

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 приложений "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 приложениях "Лаборатории Касперского". Например, общее событие Вирусная атака. Общие события имеют строго определенные синтаксис и семантику. Общие события используются, например, в отчетах и панели мониторинга.
- Специфические события управляемых приложений "Лаборатории Касперского". Каждое управляемое приложение "Лаборатории Касперского" имеет собственный набор событий.

События по источнику

Просмотреть полный список событий, которые может генерировать приложение, можно на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть список событий в свойствах Сервера администрирования.

События могут генерироваться следующими приложениями:

- Компоненты приложения Kaspersky Security Center Linux:
  - Сервер администрирования
  - Агент администрирования
- Управляемые приложения "Лаборатории Касперского"

  Подробнее о событиях, генерируемых управляемыми приложениями "Лаборатории Касперского", см. в документации соответствующего приложения.

События по уровню важности

Каждое событие имеет собственный уровень важности. В зависимости от условий возникновения, событию могут быть присвоены различные уровни важности. Существует четыре уровня важности событий:

- *Критическое событие* – событие, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.
- *Отказ функционирования* – событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы приложения или выполнения процедуры.
- *Предупреждение* – событие, не обязательно являющееся серьезным, однако указывающее на возможное возникновение проблемы в будущем. Чаще всего события относятся к Предупреждениям, если после их возникновения работа приложения может быть восстановлена без потери данных или функциональных возможностей.
- *Информационное сообщение* – событие, возникающее с целью информирования об успешном выполнении операции, корректной работе приложения или завершении процедуры.

Для каждого события задано время хранения, которое можно посмотреть или изменить в Kaspersky Security Center 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 компонентов 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 и Агенте администрирования. Типы событий, которые возникают в приложениях "Лаборатории Касперского", в этом разделе не перечислены.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

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 с уровнем важности **Критическое**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Срок действия сертификата Сервера администрирования для мобильных устройств истек	6129	KLSRV_EV_SRV_CERT_EXPIRED_DN	События этого типа возникают, если истек срок действия сертификатов Сервера администрирования для мобильных устройств и для устройств с защитой на уровне UEFI в сети. Вам необходимо обновить сертификат, срок действия которого истек.	180 дней
Аудит: Не удалось выполнить экспорт в SIEM-систему	5130	KLAUD_EV_SIEM_EXPORT_ERROR	События этого типа возникают при сбое экспорта событий в SIEM-систему из-за ошибки соединения с SIEM-системой.	180 дней
Устройство стало неуправляемым	4111	KLSRV_HOST_OUT_CONTROL	События этого типа возникают, если управляемое устройство видимо в сети, но не подключено к Серверу администрирования в течение заданного периода. Определите, что мешает правильной работе Агента администрирования на устройстве. Возможные причины могут включать проблемы сети и удаление Агента администрирования с устройства.	180 дней
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

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
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 Linux проверяет, не истек ли срок действия лицензии. События этого типа публикуются за 30 дней, 15 дней, 5 дней и 1 день, до истечения срока действия лицензии. Это количество дней невозможно изменить. Если Сервер администрирования выключен, в указанный день окончания срока действия лицензии, событие не будет опубликовано до следующего дня. После окончания срока действия коммерческой лицензии, Kaspersky Security Center 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
Лицензионное ограничение превышено	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Один раз в день Kaspersky Security Center Linux проверяет, не превышены ли лицензионные ограничения. События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии превышает 110% от общего количества лицензионных единиц, 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 действительный код активации или файл ключа на Сервер администрирования). Kaspersky Security Center Linux определяет правила генерации событий при превышении лицензионного ограничения.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Режим ограниченной функциональности	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	События этого типа возникают, если Kaspersky Security Center Linux начинает работать в режиме базовой функциональности, без поддержки Управления мобильными устройствами и Системного администрирования. Ниже приведены причины и соответствующие ответы на событие: • Срок действия лицензии истек. Предоставьте лицензию на полную функциональность Kaspersky Security Center Linux (добавьте действительный код активации или файл ключа на Сервер администрирования). • Сервер администрирования управляет большим количеством устройств, чем может использоваться по предоставленной лицензии. Переместите устройства из состава групп администрирования одного Сервера в группы администрирования другого Сервера (если лицензионное ограничение другого Сервера не превышено).	180 дней
Срок действия MDM-сертификата истек	4132	KLSRV_CERTIFICATE_EXPIRED	События этого типа возникают, если истек срок действия клиентского сертификата на мобильных устройствах.	180 дней
Файл ключа добавлен в список запрещенных	4124	KLSRV_LICENSE_BLACKLISTED	События этого типа возникают, если "Лаборатория Касперского" добавила код активации или файл ключа, который вы используете, в список запрещенных. Обратитесь в Службу технической поддержки для получения подробной информации.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Обновления модулей приложений "Лаборатории Касперского" отозваны	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	События этого типа возникают, если обновления были отозваны техническими специалистами "Лаборатории Касперского", например, по причине их замены на более новые версии. Для таких обновлений отображается статус *Отозвано*. Событие не относится к патчам Kaspersky Security Center Linux и не относится к модулям управляемых приложений "Лаборатории Касперского". Событие содержит причину, из-за которой обновления не установлены.	180 дней
Вирусная атака	• 26 (для компонента Защита от файловых угроз) • 27 (для компонента Защита от почтовых угроз) • 28 (для сетевого экрана)	GNRL_EV_VIRUS_OUTBREAK	События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения. Вы можете ответить на событие следующими способами: • Настройте пороговые значения в свойствах Сервера администрирования. • Создайте более строгую политику, которая будет активирована, или создайте задачу, которая будет запускаться при возникновении этого события.	

События отказа функционирования Сервера администрирования

В таблице ниже приведены события Сервера администрирования с уровнем важности **Отказ функционирования**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
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: • Проверить, 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. • Проверить подключение к интернету, так как это может быть причиной события. Следуйте инструкциям по обновлению баз и модулей приложений.	180 дней
Не удалось выполнить опрос облачного сегмента	4143	KLSRV_KLCLOUD_SCAN_ERROR	События этого типа возникают, если Сервер администрирования не может опросить сегмент сети в облачном окружении. Прочтите информацию в описании события и отреагируйте соответствующим образом.	Не хранится
Для одной из групп лицензионных приложений превышено ограничение числа установок	4126	KLSRV_INVLICPROD_EXCEDED	Сервер администрирования генерирует события такого типа периодически (каждый час). События этого типа возникают, если в Kaspersky Security Center Linux вы управляете лицензионными ключами приложений сторонних производителей и если количество установок превысило заданное в лицензионном ключе приложения стороннего производителя ограничение. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите приложение стороннего производителя с устройств, на которых оно не используется. • Используйте лицензию стороннего производителя на большее количество устройств. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений. В группу лицензионных приложений входят приложения сторонних производителей, отвечающие заданным вами критериям.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Нет свободного места на диске	4107	KLSRV_DISK_FULL	События этого типа возникают, если на жестком диске устройства, на котором установлен Сервер администрирования, заканчивается дисковое пространство. Освободите дисковое пространство на устройстве.	180 дней
Недостаточно места в базе данных Сервера администрирования	4110	KLSRV_DATABASE_FULL	События этого типа возникают, если нет свободного места в базе Сервера администрирования. Сервер администрирования не работает, если его база данных переполнена и дальнейшая запись в базу данных невозможна. Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие: • Ограничьте количество событий, хранящихся в базе данных Сервера администрирования. • В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль приложений. Вы можете изменить параметры политики Kaspersky Endpoint Security, касающиеся хранения событий компонента Контроль приложений в базе данных Сервера администрирования. Просмотрите информацию о выборе СУБД.	180 дней
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
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

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
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 установлена СУБД. • Просмотрите журналы событий СУБД и найдите причину недоступности базы Сервера администрирования.	180 дней

События предупреждения Сервера администрирования

В таблице ниже приведены события Сервера администрирования с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. 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.

События предупреждения Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Срок действия сертификата Сервера администрирования для мобильных устройств истекает	6128	KLSRV_EV_SRV_CERT_EXPIRES_SOON	События этого типа возникают, если истек срок действия сертификатов Сервера администрирования для мобильных устройств и для устройств с защитой на уровне UEFI в сети. Вам необходимо обновить сертификат, срок действия которого истек.	90 дней
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
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

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Аудит: Не удалось выполнить тестовое подключение к SIEM-серверу	5120	KLAUD_EV_SIEM_TEST_FAILED	События этого типа возникают при сбое автоматической проверки подключения к SIEM-серверу.	90 дней
Сертификат удален	4134	KLSRV_CERTIFICATE_REMOVED	События этого типа возникают, если администратор удаляет сертификат любого типа (общий, почтовый, VPN) для Управления мобильными устройствами. После удаления сертификата мобильные устройства, подключенные по этому сертификату, не смогут подключиться к Серверу администрирования. Это событие может быть полезно при исследовании неисправностей, связанных с Управлением мобильными устройствами.	90 дней
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**. Это могло произойти из-за ошибки, которая возникла при создании сертификата. Может потребоваться перевыпуск сертификата вручную. • Если вы используете интеграцию с инфраструктурой открытых ключей, причиной может быть отсутствие атрибута SAM-Account-Name учетной записи, которая используется для интеграции с PKI и для выпуска сертификата. Просмотрите свойства учетной записи.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Конфликт имен устройств	4102	KLSRV_EVENT_HOSTS_CONFLICT	События этого типа возникают, если Сервер администрирования рассматривает два или более управляемых устройства как одно устройство. Чаще всего это происходит, когда клонированный жесткий диск использовался для развертывания приложений на управляемых устройствах и без переключения Агента администрирования в режим клонирования выделенного диска на эталонном устройстве. Чтобы избежать этой проблемы, перед клонированием жесткого диска этого устройства переключите Агент администрирования в режим клонирования диска на эталонном устройстве.	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
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

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Устройство долго не проявляет активности в сети	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	События этого типа возникают, если управляемое устройство неактивно в течение некоторого времени. Чаще всего это происходит, когда управляемое устройство выводится из эксплуатации. Вы можете ответить на событие следующими способами: • Удалите устройство из списка управляемых устройств вручную. Укажите интервал, по истечении которого создается событие **Устройство долго не проявляет активности в сети** с помощью Kaspersky Security Center Web Console. • Укажите интервал, по истечении которого устройство автоматически удаляется из группы с помощью Kaspersky Security Center Web Console.	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
Не удалось скачать файл на устройство	4165	KLSRV_FILE_DOWNLOAD_FAILED	События этого типа возникают в следующих случаях: • Вы пытаетесь загрузить файл в корпоративный контейнер, но корпоративный контейнер не был создан. • На устройстве недостаточно места. • Не удалось скачать информацию о файле с сервера. • Не удалось скачать содержимое файла с сервера. • Не удалось создать папку на устройстве. • На личном устройстве отсутствует доступ к файлам. • В корпоративном контейнере отсутствует доступ к файлу.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось отправить FCM-сообщение на FCM-сервер	4140	KLSRV_GCM_GENERAL_ERROR	События этого типа возникают из-за непредвиденных ошибок на стороне Сервера администрирования при работе с HTTP-протоколом Google Firebase Cloud Messaging. Прочтите информацию в описании события и отреагируйте соответствующим образом. Если вы не можете найти решение проблемы самостоятельно, рекомендуем вам обратиться в Службу технической поддержки "Лаборатории Касперского".	90 дней
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
Обнаружено получение частных событий		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
Жесткий диск почти заполнен	4105	KLSRV_NO_SPACE_ON_VOLUMES	События этого типа возникают, если на устройстве, на котором установлен Сервер администрирования, почти закончилось дисковое пространство. Освободите дисковое пространство на устройстве.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
HTTP-ошибка при отправке FCM-сообщения на FCM-сервер	4139	KLSRV_GCM_HTTP_ERROR	События этого типа возникают, если Управление мобильными устройствами настроено на использование Google Firebase Cloud Messaging (FCM) для подключения управляемых мобильных устройств с операционной системой Android, а FCM-сервер возвращает запрос Серверу администрирования с кодом HTTP, отличным от 200 (OK). Ниже приведены возможные причины событий и соответствующие действия по реагированию на событие: • Проблемы на стороне FCM-сервера. Прочтите HTTP код в описании события и ответьте соответствующим образом. Дополнительная информация о HTTP кодах, полученных от FCM-сервера, и связанных с ними ошибках есть в документации службы Google Firebase (см. главу "Downstream message error response codes"). • Проблемы на стороне прокси-сервера (если вы используете прокси-сервер). Прочтите HTTP код в описании события и ответьте соответствующим образом.	90 дней
Лицензионное ограничение превышено	4098	KLSRV_EV_LICENSE_CHECK_100_110	Один раз в день Kaspersky Security Center Linux проверяет, не превышены ли лицензионные ограничения. События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии 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 действительный код активации или файл ключа на Сервер администрирования). Kaspersky Security Center Linux определяет правила генерации событий при превышении лицензионного ограничения.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Для одной из групп лицензионных приложений скоро будет достигнуто ограничение числа установок	4128	KLSRV_INVLICPROD_EXPIRED_SOON	События этого типа возникают, когда истекает срок действия одного из лицензионных ключей сторонних приложений, входящих в группу лицензионных приложений. В результате число разрешенных установок для одной из групп будет уменьшено. Вы можете ответить на событие следующими способами: • Если приложение стороннего производителя не используется на каких-то управляемых устройствах, удалите приложение с этих устройств. • Если вы ожидаете, что количество установок для приложения стороннего производителя превысит разрешенное ограничение в ближайшем будущем, рассмотрите возможность получения лицензии приложения стороннего производителя на большее количество устройств заранее. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений.	90 дней
Зарегистрированы новые обновления модулей приложений "Лаборатории Касперского"	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	События этого типа возникают, если Сервер администрирования регистрирует новые обновления приложений "Лаборатории Касперского", установленных на управляемых устройствах, для установки которых требуется одобрение. Одобрите или отклоните обновления с помощью Kaspersky Security Center Web Console.	90 дней
Недостаточно места в базе данных Сервера администрирования	4106	KLSRV_NO_SPACE_IN_DATABASE	События этого типа возникают, если свободное место в базе Сервера администрирования ограничено. Если вы не устраните эту проблему, скоро база данных Сервера администрирования достигнет своей емкости и Сервер администрирования не будет работать. Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие. • Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования. • Сократите список событий для хранения в базе данных Сервера администрирования. Просмотрите информацию о выборе СУБД.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Превышено ограничение числа событий, началось удаление событий из базы данных	4145	KLSRV_EVP_DB_TRUNCATING	События такого типа возникают, если удаление старых событий из базы данных Сервера администрирования началось после достижения максимального количества событий, хранящихся в базе данных Сервера администрирования. 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.	Не хранится
Превышено ограничение числа событий, удалены события из базы данных	4146	KLSRV_EVP_DB_TRUNCATED	События такого типа возникают, если старые события удалены из базы данных Сервера администрирования после достижения максимального количества событий, хранящихся в базе данных Сервера администрирования. 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 с уровнем важности **Информационное сообщение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	У
Срок действия сертификата Сервера администрирования для мобильных устройств обновлен	6127	KLSRV_EV_SRV_CERT_RENEWED	События этого типа возникают, если сертификат Сервера администрирования был обновлен.	3
Аудит: Команда была отправлена на устройство	4170	KLAUD_EV_COMMAND_SENT	События этого типа возникают, если пользователь отправил команду на мобильное устройство.	3
Аудит: Подключение к Серверу администрирования было прервано	4151	KLAUD_EV_SERVERDISCONNECT		3
Аудит: Подключение к Серверу администрирования	4147	KLAUD_EV_SERVERCONNECT	События этого типа возникают при подключении пользователя к Серверу администрирования с помощью Kaspersky Security Center Web Console. Такие события включают информацию об IP-адресе устройства, на котором установлен Сервер Kaspersky Security Center Web Console.	3
Аудит: Пользовательский параметр создан	4167	KLAUD_EV_CUSTOM_PARAMETER_CREATED	События этого типа возникают, если пользователь создал новый пользовательский параметр.	3
Аудит: Пользовательский параметр удален	4168	KLAUD_EV_CUSTOM_PARAMETER_DELETED	События этого типа возникают, если пользователь удалил пользовательский параметр.	3
Аудит: Настройки пользовательского параметра изменены	4169	KLAUD_EV_CUSTOM_PARAMETER_CHANGED	События этого типа возникают, если пользователь изменил настройки пользовательского параметра.	3
Аудит: Значения пользовательских параметров изменены	4166	KLAUD_EV_CUSTOM_PARAMETERS_VALUE_CHANGED_BY_ADMIN	События этого типа возникают, если пользователь задал или изменил значения одного или нескольких пользовательских параметров на Android-устройстве с помощью Kaspersky Security Center Web Console.	3
Аудит: Ключи шифрования импортированы/ экспортированы	5100	KLAUD_EV_DPEKEYSEXPORT	Например, это событие происходит во время переноса данных.	3

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	У
Аудит: Изменение параметров группы	4149	KLAUD_EV_ADMGROUP_CHANGED	События этого типа возникают при изменении группы безопасности.	3
Аудит: Изменение объекта	4148	KLAUD_EV_OBJECTMODIFY	Это событие отслеживает изменения в следующих объектах: • группах администрирования; • группах безопасности; • пользователях; • управляемых устройствах; • инсталляционных пакетах; • задачах; • политиках; • Серверах; • виртуальных Серверах.	3
Аудит: Свойства объекта были изменены	4152	KLAUD_EV_OBJECTPROPMODIFIED	Это событие отслеживает изменения в следующих параметрах: • пользователь; • лицензия; • Сервер; • виртуальный Сервер.	3
Аудит: Изменение статуса объекта	4150	KLAUD_EV_TASK_STATE_CHANGED	Например, это событие возникает, если задача завершилась ошибкой.	3
Аудит: Тестовое подключение к SIEM-серверу выполнено успешно	5110	KLAUD_EV_SIEM_TEST_SUCCESS	События этого типа возникают при успешном подключении к SIEM-серверу.	3
Аудит: Права пользователя были изменены	4153	KLAUD_EV_OBJECTACLMODIFIED	События этого типа возникают, если права пользователя были изменены.	3
Установлено соединение с главным Сервером администрирования	4117	KLSRV_EV_MASTER_SRV_CONNECTED		3
Установлено соединение с подчиненным Сервером администрирования	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	Подробнее см. в статье Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования.	3

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	У
Базы обновлены	4144	KLSRV_UPD_BASES_UPDATED	События этого типа возникают, когда задача **Загрузка обновлений в хранилище Сервера администрирования** завершает обновление базы данных.	3
Устройство было автоматически перемещено с помощью правила	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	События этого типа возникают, если устройства были перемещены в группы администрирования в соответствии с правилами перемещения устройств. Для каждого перемещенного устройства публикуется отдельное событие.	3
Устройство удалено из группы: долгое отсутствие активности в сети	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	События этого типа возникают, когда устройства были автоматически удалены из группы из-за неактивности.	3
Идентификатор экземпляра FCM мобильного устройства изменен	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	События этого типа возникают при изменении токена Firebase Cloud Messaging на устройстве. Информацию о ротации токенов FCM см. в документации сервиса Firebase.	3
Файл загружен на Сервер администрирования	4162	KLSRV_FILE_UPLOADED	События этого типа возникают, если администратор загрузил файл в список в Web Console: **Управление активами** → **Мобильные** → **Приложения и файлы** → **Файлы**.	3
Файл удален с Сервера администрирования	4163	KLSRV_FILE_REMOVED	События этого типа возникают, если администратор удалил файл из списка в Web Console: **Управление активами** → **Мобильные** → **Приложения и файлы** → **Файлы**.	3

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	У
Файл загружен на устройство	4164	KLSRV_FILE_DOWNLOADED	События этого типа возникают в следующих случаях: • Администратор загрузил файл на свое рабочее место из списка в Web Console: **Управление активами → Мобильные → Приложения и файлы → Файлы**. • Файл из списка **Управление активами → Мобильные → Приложения и файлы → Файлы** загружен на устройство, на котором установлено приложение Kaspersky Endpoint Security для Android.	3
Не удалось загрузить файл на устройство	4165	KLSRV_FILE_DOWNLOAD_FAILED	События этого типа возникают в следующих случаях: • Произошла ошибка при попытке администратора загрузить файл на свое рабочее место из списка в Web Console: **Управление активами → Мобильные → Приложения и файлы → Файлы**. • Произошла ошибка при загрузке файла из списка **Управление активами → Мобильные → Приложения и файлы → Файлы** на устройство, на котором установлено приложение Kaspersky Endpoint Security для Android.	3
Появились файлы для отправки на анализ в "Лабораторию Касперского"	4131	KLSRV_APS_FILE_APPEARED		3

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	У
Для одной из групп лицензионных приложений число разрешенных установок исчерпано более чем на 90%	4127	KLSRV_INVLICPROD_FILLED	События этого типа возникают, если количество установок приложений сторонних производителей, включенных в группу лицензионных приложений, достигает 90% от максимально допустимого значения, указанного в свойствах лицензионного ключа. Вы можете ответить на событие следующими способами: • Если приложение стороннего производителя не используется на каких-то управляемых устройствах, удалите приложение с этих устройств. • Если вы ожидаете, что количество установок для приложения стороннего производителя превысит разрешенное ограничение в ближайшем будущем, рассмотрите возможность получения лицензии приложения стороннего производителя на большее количество устройств заранее. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений.	3
Обнаружено новое устройство	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	События этого типа возникают при обнаружении новых сетевых устройств.	3

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	У
Лицензионный ключ использован более чем на 90%	4097	KLSRV_EV_LICENSE_CHECK_90	События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии превышает 90% от общего количества лицензионных единиц, охватываемых лицензией. Даже при превышении лицензионных ограничений 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 действительный код активации или файл ключа на Сервер администрирования). Kaspersky Security Center Linux определяет правила генерации событий при превышении лицензионного ограничения.	3
Резервный сертификат Сервера администрирования для мобильных устройств создан	6126	KLSRV_EV_SRV_CERT_RESERVE_CREATED	События этого типа возникают, если сертификат Сервера администрирования создан.	3
Обновления успешно скопированы в заданную папку	4122	KLSRV_UPD_REPL_OK	События этого типа возникают, когда задача **Загрузка обновлений в хранилище Сервера администрирования** завершает копирование файлов в указанную папку.	3

События **Резервный сертификат создан** и **Сертификат обновлен** автоматически публикуются Сервером администрирования и отображаются в Консоли администрирования только при выполнении соответствующих этим событиям операций для сертификатов Сервера администрирования для мобильных устройств и устройств с защитой на уровне UEFI.

События Агента администрирования

В этом разделе содержится информация о событиях Агента администрирования.

События отказа функционирования Агента администрирования

В таблице ниже приведены события Агента администрирования Kaspersky Security Center Linux с уровнем важности **Отказ функционирования**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

События отказа функционирования Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось установить корневые сертификаты	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	Событие содержит описание ошибки установки сертификатов.	30 дней
Не удалось установить обновление стороннего производителя	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	События этого типа возникают, если используются возможности Системного администрирования, и если обновление программного обеспечения сторонних производителей прошло неуспешно. Проверьте, корректна ли ссылка на приложение стороннего производителя. Прочтите описание события.	30 дней
Не удалось установить обновления Windows	7717	KLNAG_EV_WUA_INSTALL_ERROR	События этого типа возникают, если обновления Центра обновления Windows были неуспешными. Прочтите описание события. Поищите описание ошибки в базе знаний Microsoft. Обратитесь в службу технической поддержки Microsoft, если вы не можете решить проблему самостоятельно.	30 дней
Не удалось удалить корневые сертификаты	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	Событие содержит описание ошибки удаления сертификатов.	30 дней
Не удалось восстановить файл sudoers до референсного значения	7726	KLNAG_EV_SUDOER_RESTORED_ERR	Событие содержит описание ошибки замены файла sudoers.	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Ошибка при установке обновления	7702	KLNAG_EV_PATCH_INSTALL_ERROR	События этого типа возникают, если автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center Linux прошла неуспешно. Событие не относится к обновлениям управляемых приложений "Лаборатории Касперского". Прочтите описание события. Причиной этого события может быть проблема операционной системы Windows на Сервере администрирования. Если в описании упоминается какая-либо проблема конфигурации Windows, устраните эту проблему.	30 дней
Управление учетными записями: ошибки	7723	KLNAG_EV_USR_MNG_ERR	Общее событие предупреждения.	30 дней

События предупреждения Агента администрирования

В таблице ниже приведены события Агента администрирования с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

События предупреждения Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Прокси-сервер KSN был запущен. Не удалось проверить доступность KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	События этого типа возникают при сбое тестового соединения для настроенного подключения прокси-сервера KSN.	30 дней
Произошла проблема безопасности	549	GNRL_EV_APP_INCIDENT_OCCURED	События этого типа возникают при обнаружении инцидента на устройстве. Например, это событие возникает, когда на устройстве мало места на диске.	30 дней
Обнаружен файл sudoers, который не соответствует референсному значению	7724	KLNAG_EV_SUDOER_DIFFERENT	События этого типа возникают, если есть несовпадение между файлом sudoers и референсным файлом.	30 дней
Установка обновления стороннего программного обеспечения отложена	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	Например, события этого типа возникают, когда отклоняется Лицензионное соглашение для установки обновлений приложений сторонних производителей.	30 дней
Установка обновления стороннего ПО завершена с предупреждением	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	Скачайте файлы трассировки и проверьте значение поля KLRI_PATCH_RES_DESC.	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Управление учетными записями: предупреждения	7722	KLNAG_EV_USR_MNG_WRN	Общее событие предупреждения.	30 дней
Возвращено предупреждение во время установки обновления модулей приложений	7701	KLNAG_EV_PATCH_INSTALL_WARNING	Скачайте файлы трассировки и проверьте значение поля KLRI_PATCH_RES_DESC.	30 дней

Информационные события Агента администрирования

В таблице ниже приведены события Агента администрирования с уровнем критичности **Информационное сообщение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Информационные события Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Установлено приложение	7703	KLNAG_EV_INV_APP_INSTALLED	30 дней
Приложение удалено	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 дней
Получен сертификат для HTTPS-порта Веб-сервера	—	WEB_SERVER_CERTIFICATE_RENEWED	30 дней
Устройство авторизовано	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 дней
Обнаружено новое устройство	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 дней
Устройство удалено	7709	KLNAG_EV_DEVICE_REMOVE	30 дней
Запущена установка обновления модулей приложений	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 дней
Прокси-сервер KSN был запущен. Проверка доступности KSN прошла успешно	7719	KSNPROXY_STARTED_CON_CHK_OK	30 дней
Прокси-сервер KSN остановлен	7720	KSNPROXY_STOPPED	30 дней
Установлено наблюдаемое приложение	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 дней
Удалено наблюдаемое приложение	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 дней
Новое устройство добавлено	7708	KLNAG_EV_DEVICE_ARRIVAL	30 дней
Корневой сертификат установлен	7727	KLNAG_EV_ROOT_CERT_INSTALLED	30 дней
Корневые сертификаты удалены	7729	KLNAG_EV_ROOT_CERT_REMOVED	30 дней
Файл sudoers успешно восстановлен до референсного значения	7725	KLNAG_EV_SUDOER_RESTORED	30 дней
Установлено стороннее приложение	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 дней
Обновление для приложений стороннего производителя установлено успешно	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 дней
Запущена установка обновления стороннего ПО	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Обновление модулей приложений успешно установлено	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 дней
Управление учетными записями: информационные сообщения	7721	KLNAG_EV_USR_MNG_INF	30 дней
Веб-Сервер запущен на устройстве	—	WEB_SERVER_STARTED	30 дней
Веб-Сервер остановлен на устройстве	—	WEB_SERVER_STOPPED	30 дней
Совместный доступ к рабочему столу Windows: приложение было запущено	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 дней
Совместный доступ к рабочему столу Windows: файл был изменен	7713	KLUSRLOG_EV_FILE_MODIFIED	30 дней
Совместный доступ к рабочему столу Windows: файл был прочитан	7712	KLUSRLOG_EV_FILE_READ	30 дней
Совместный доступ к рабочему столу Windows: предоставлен	7715	KLUSRLOG_EV_WDS_BEGIN	30 дней
Совместный доступ к рабочему столу Windows: завершен	7716	KLUSRLOG_EV_WDS_END	30 дней

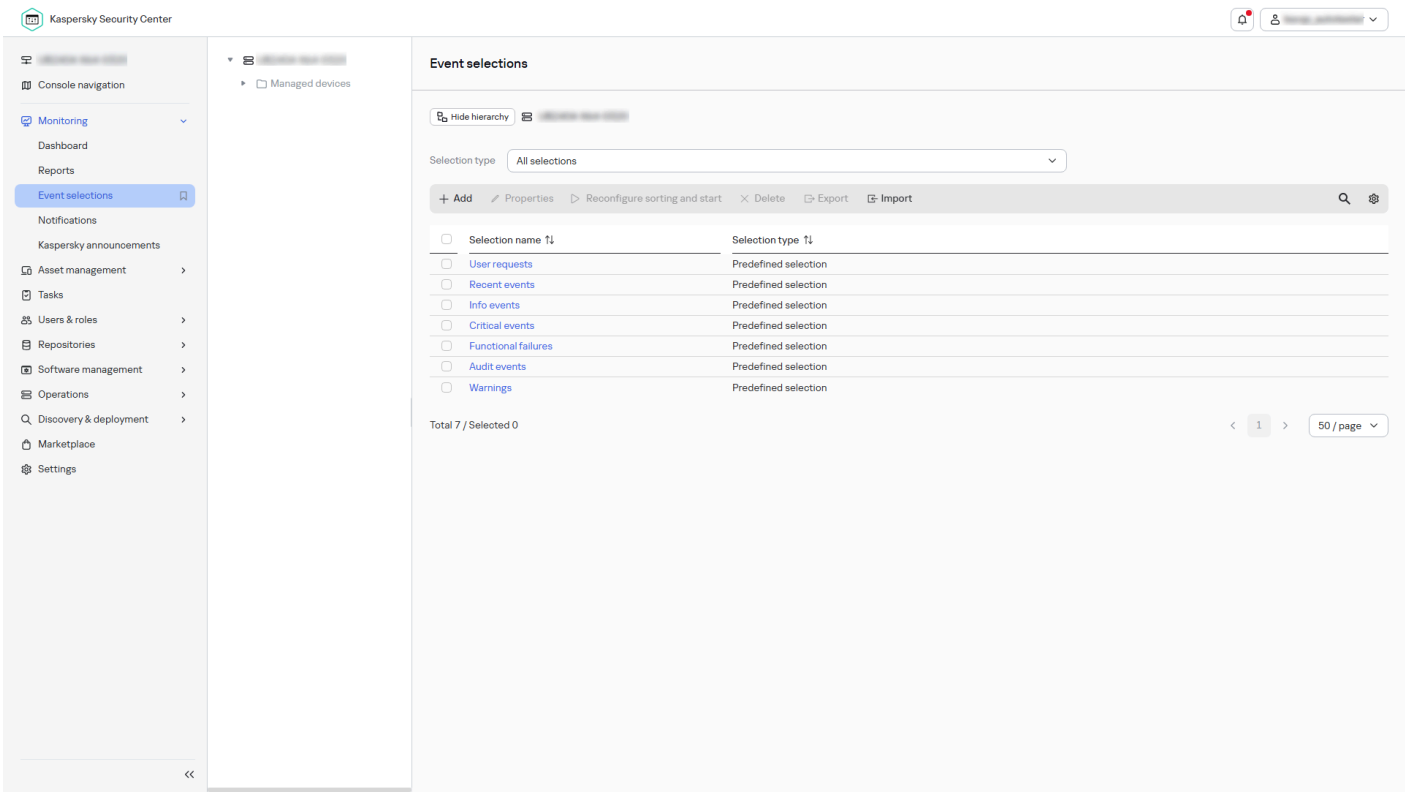
Использование выборок событий

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 Web Console.

Выборки событий доступны в Kaspersky Security Center Web Console в разделе **Мониторинг → Выборки событий**.



Список выборок 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 события.**
- **Запросы пользователей** (события управляемых приложений).
- **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 приложения и компонента, а также по временному интервалу. Также можно включить результаты задачи в область поиска. Вы также можете использовать поле поиска, в котором можно ввести слово или несколько слов. Отображаются все события, содержащие любые введенные слова в любом месте их свойств (таких как имя события, описание, имя компонента).

Как для предопределенных выборок, так и для пользовательских выборок вы можете ограничить количество отображаемых событий или количество записей для поиска. Оба варианта влияют на время, за которое Kaspersky Security Center Linux отображает события. Чем больше база данных, тем более трудоемким может быть процесс.

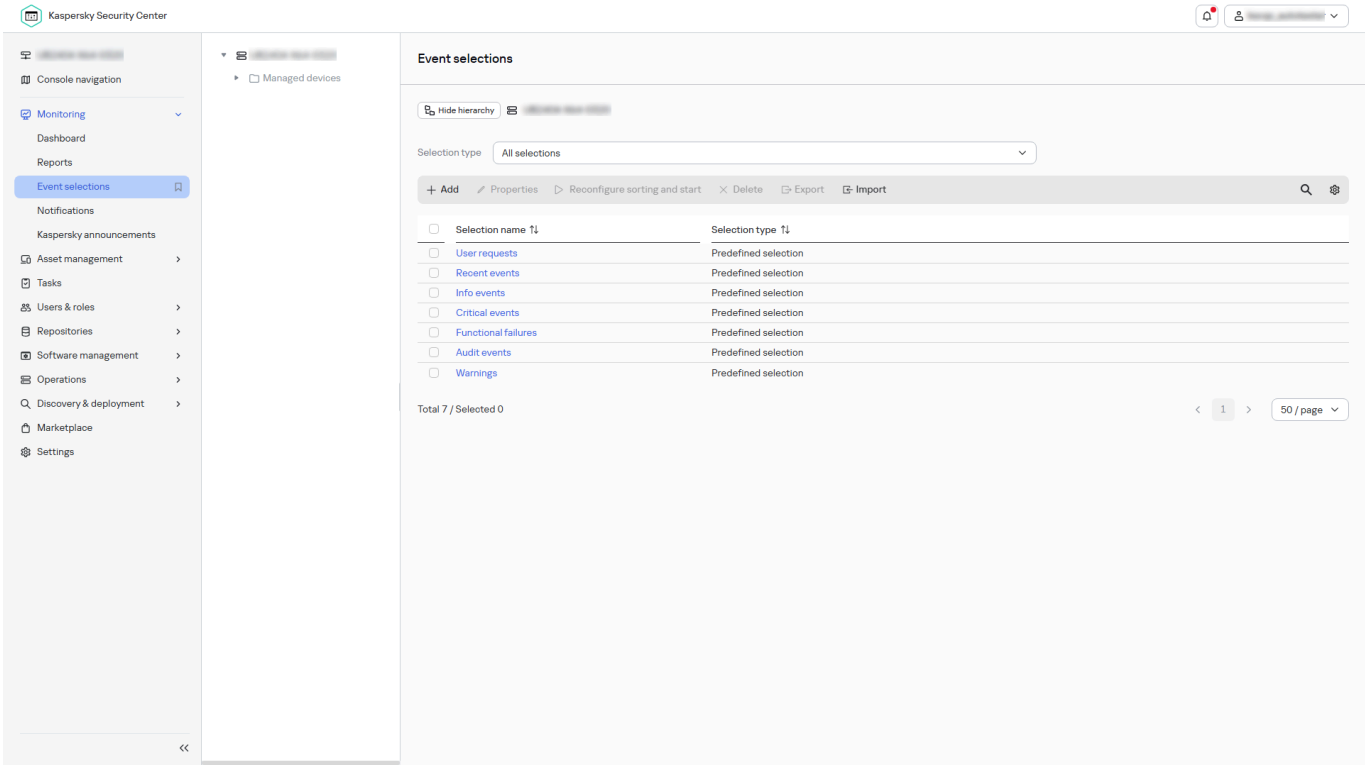
Вы можете выполнить следующее:

- 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:

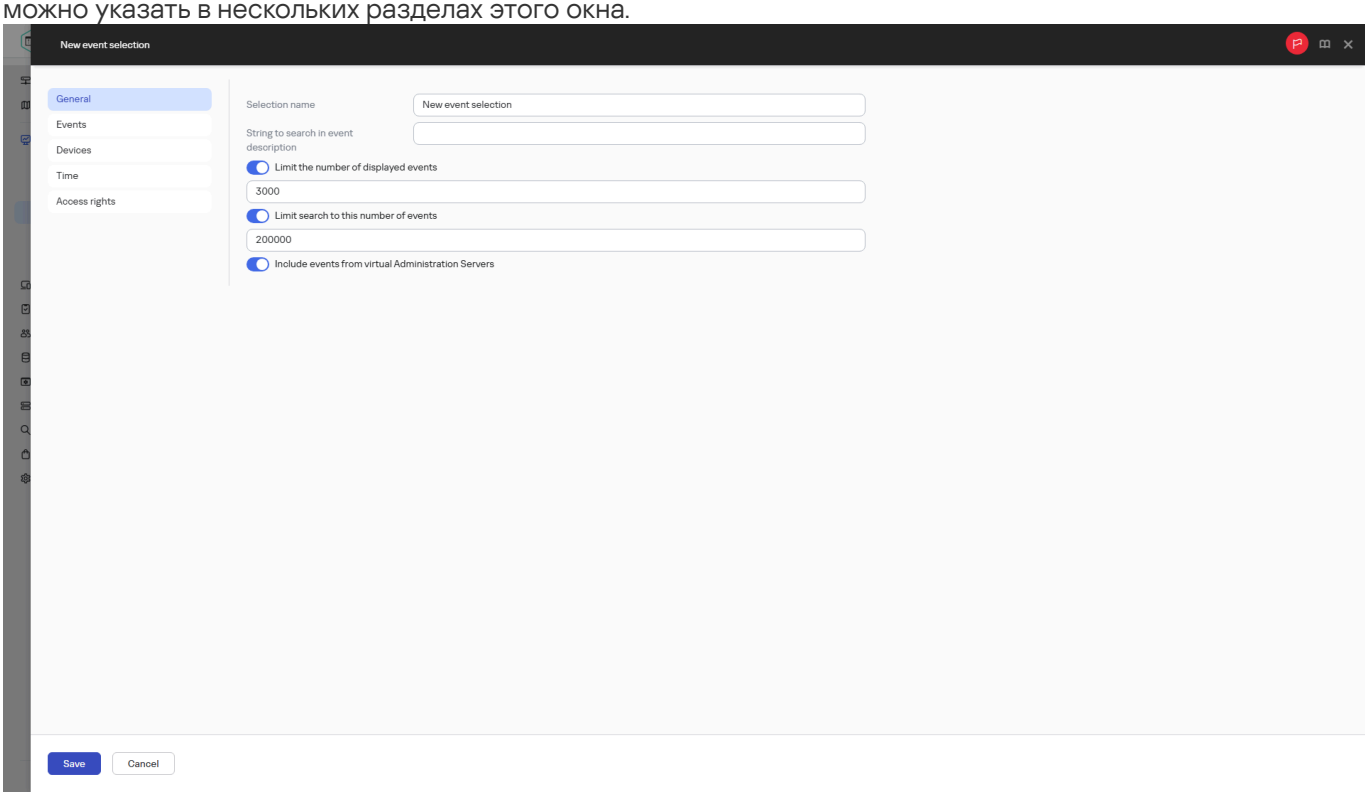
1. В главном окне приложения перейдите в раздел **Мониторинг → Выборки событий**.



Список выборок 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.



Создание выборки событий.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

   Откроется окно подтверждения.

5. Чтобы просмотреть результат выборки событий, установите флажок **Перейти к результатам выборки**.

6. Нажмите на кнопку **Сохранить**, чтобы подтвердить создание выборки событий.

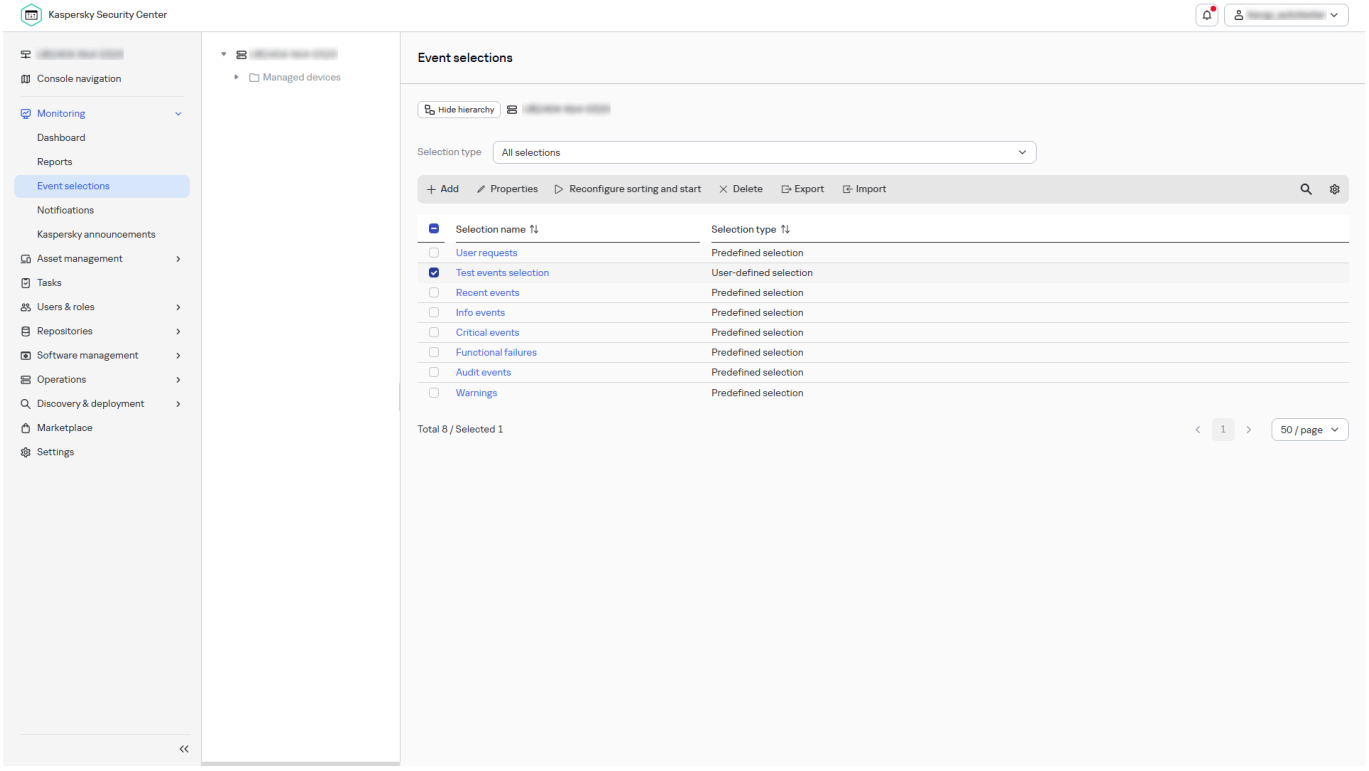
Если был установлен флажок **Перейти к результатам выборки**, результат выборки событий будет отображен на экране. В противном случае новая выборка событий появится в списке выборок событий.

Изменение выборки событий

Чтобы изменить выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Выборки событий**.

2. Установите флажок напротив выборки событий, которую требуется изменить.



Список выборок событий

3. Нажмите на кнопку **Свойства**.

   Откроется окно свойств выборки событий.

4. Отредактируйте свойства выборки событий.

   > Для стандартной выборки событий можно редактировать свойства только на следующих вкладках: **Общие** (за исключением имени выборки), **Время** и **Права доступа**.

   Для пользовательских выборок можно изменять все свойства.

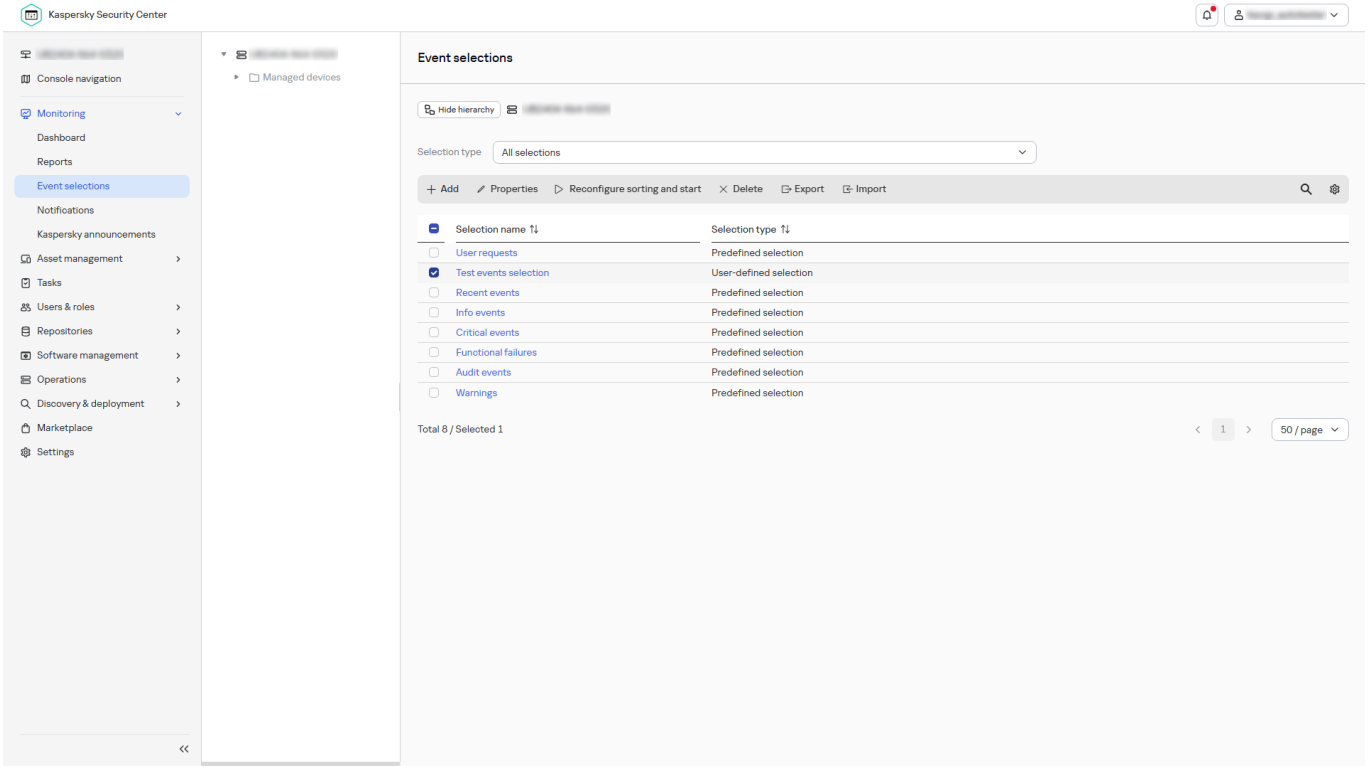
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененная выборка событий отображается в списке.

Просмотр списка выборки событий

Просмотр выборки событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется запустить.



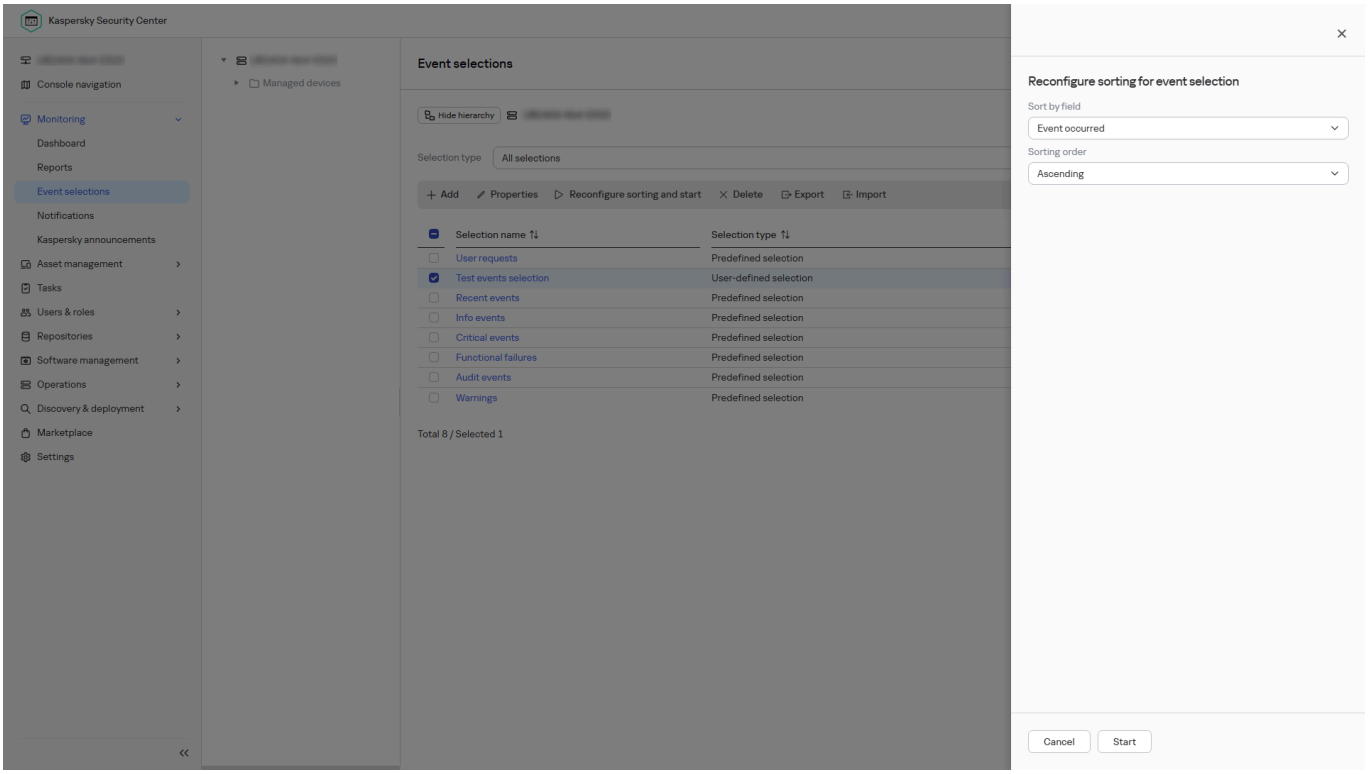
Список выборок событий

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.

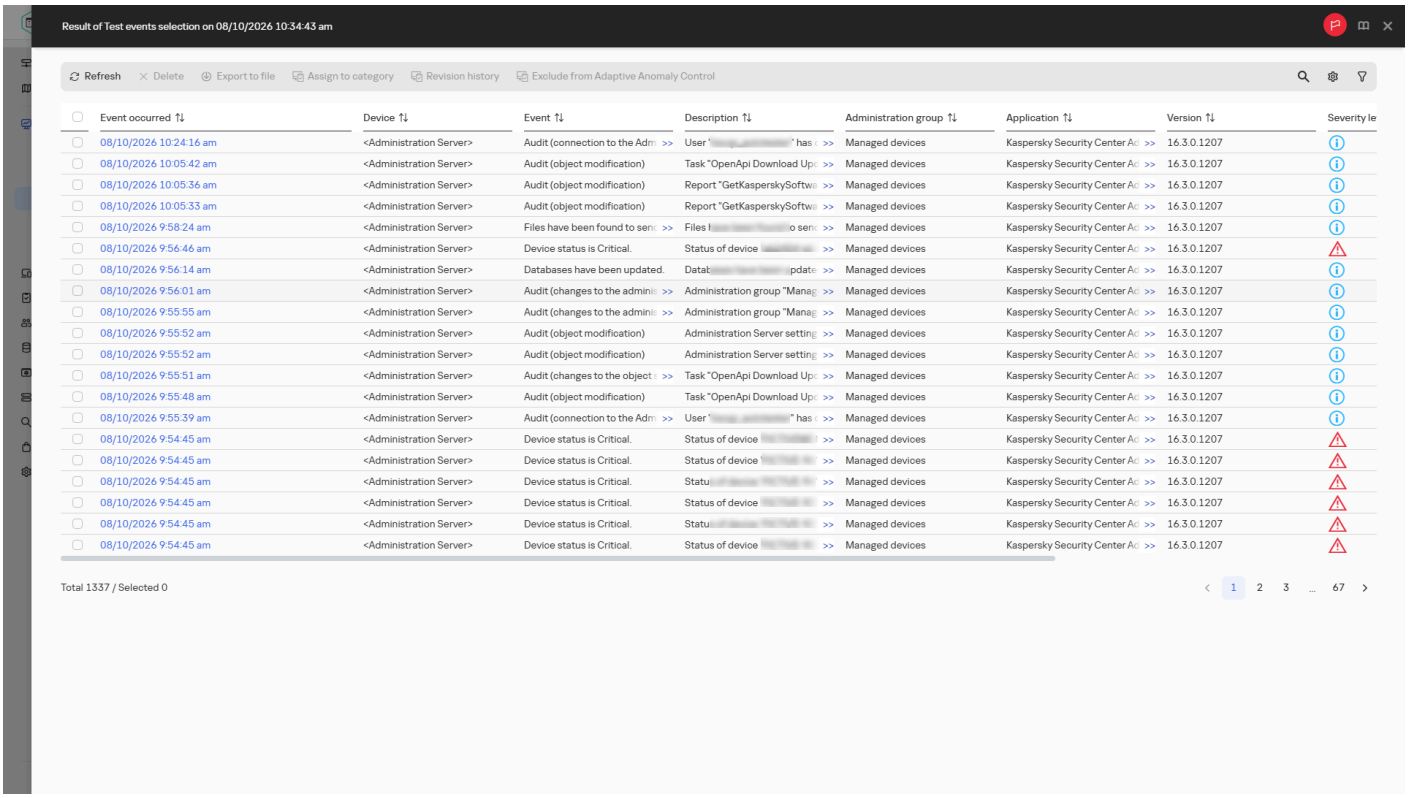


Указание параметров сортировки выборки событий

  a. 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.



Результат выборки событий

Экспорт выборки событий

Kaspersky Security Center Linux позволяет сохранить выборку событий и ее параметры в файл KLO. Вы можете использовать файл KLO для импорта сохраненной выборки событий как в Kaspersky Security Center Windows, так и в Kaspersky Security Center Linux.

Обратите внимание, что можно удалять только определенные пользователем выборки событий. Набор выборок событий, заданных по умолчанию в Kaspersky Security Center Linux (предопределенные выборки), не может быть сохранен в файл.

Чтобы экспортировать выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг → Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется экспортировать.

   Невозможно экспортировать несколько выборок событий одновременно. Если вы выберете более одной выборки, кнопка **Экспортировать** будет неактивна.
3. Нажмите на кнопку **Экспортировать**.
4. В открывшемся окне **Сохранить как** укажите имя и путь к файлу выборки событий, а затем нажмите на кнопку **Сохранить**.

   Окно **Сохранить как** отображается только в том случае, если вы используете Google Chrome, Microsoft Edge или Opera. Если вы используете другой браузер, файл выборки событий автоматически сохраняется в папку **Загрузки**.

Импорт выборки событий

Kaspersky Security Center Linux позволяет импортировать выборку событий из файла KLO. Файл KLO содержит экспортированную выборку событий и ее параметры.

Чтобы импортировать выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Выборки событий**.
2. Нажмите на кнопку **Импортировать**, чтобы выбрать файл выборки событий, который вы хотите импортировать.
3. В открывшемся окне укажите путь к файлу KLO и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл выборки событий.

   Начнется обработка выборки событий.

Появится уведомление с результатами импорта. Если выборка событий импортирована, вы можете перейти по ссылке **Просмотреть сведения об импорте**, чтобы просмотреть свойства выборки.

После успешного импорта выборка событий отображается в списке выборок. Также импортируются параметры выборки событий.

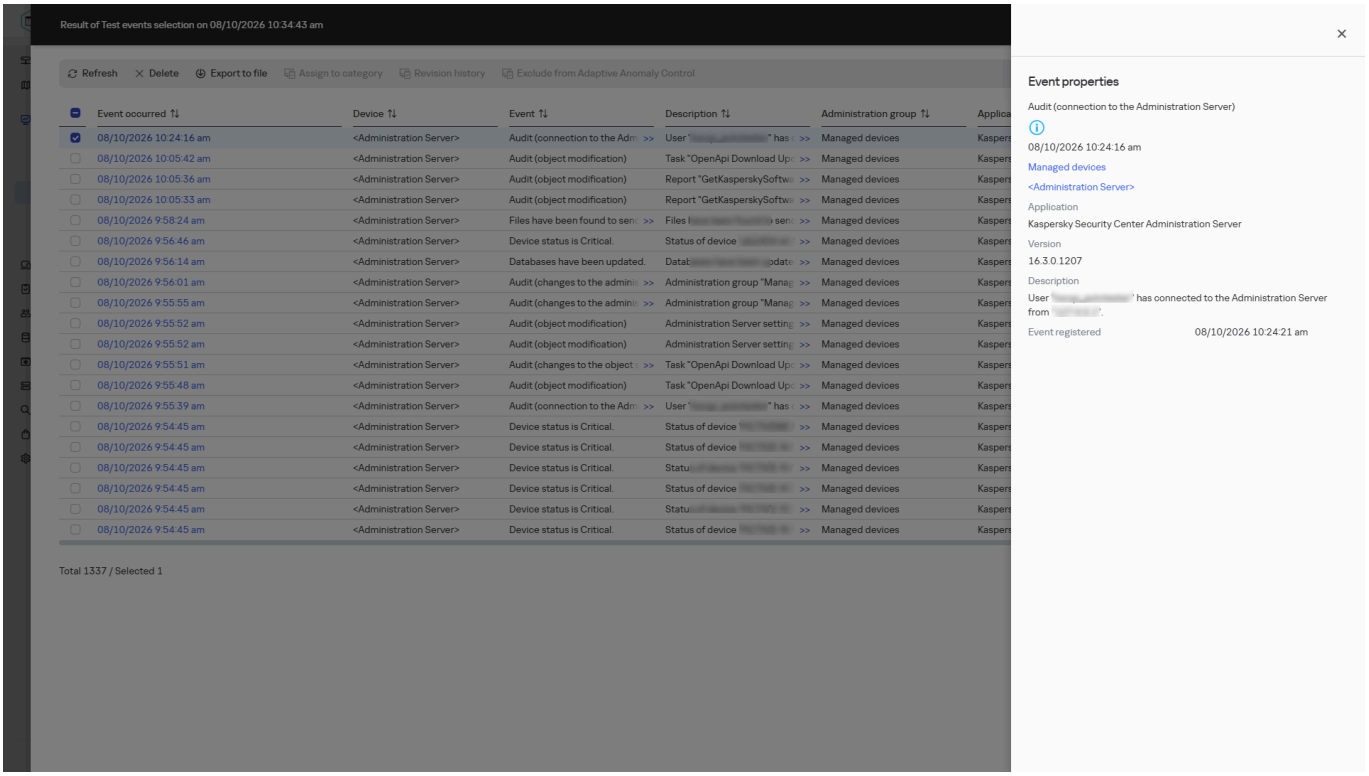
Если имя новой импортированной выборки событий идентично имени существующей выборки, имя импортированной выборки расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Просмотр информации о событии

Чтобы просмотреть детальную информацию о событии:

1. Запустите выборку событий.
2. Нажмите на требуемое событие.

Откроется окно **Свойства события**.



Окно свойств событий

3. В открывшемся окне можно выполнить следующие действия:

   - Просмотреть информацию выбранного события.
   - 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

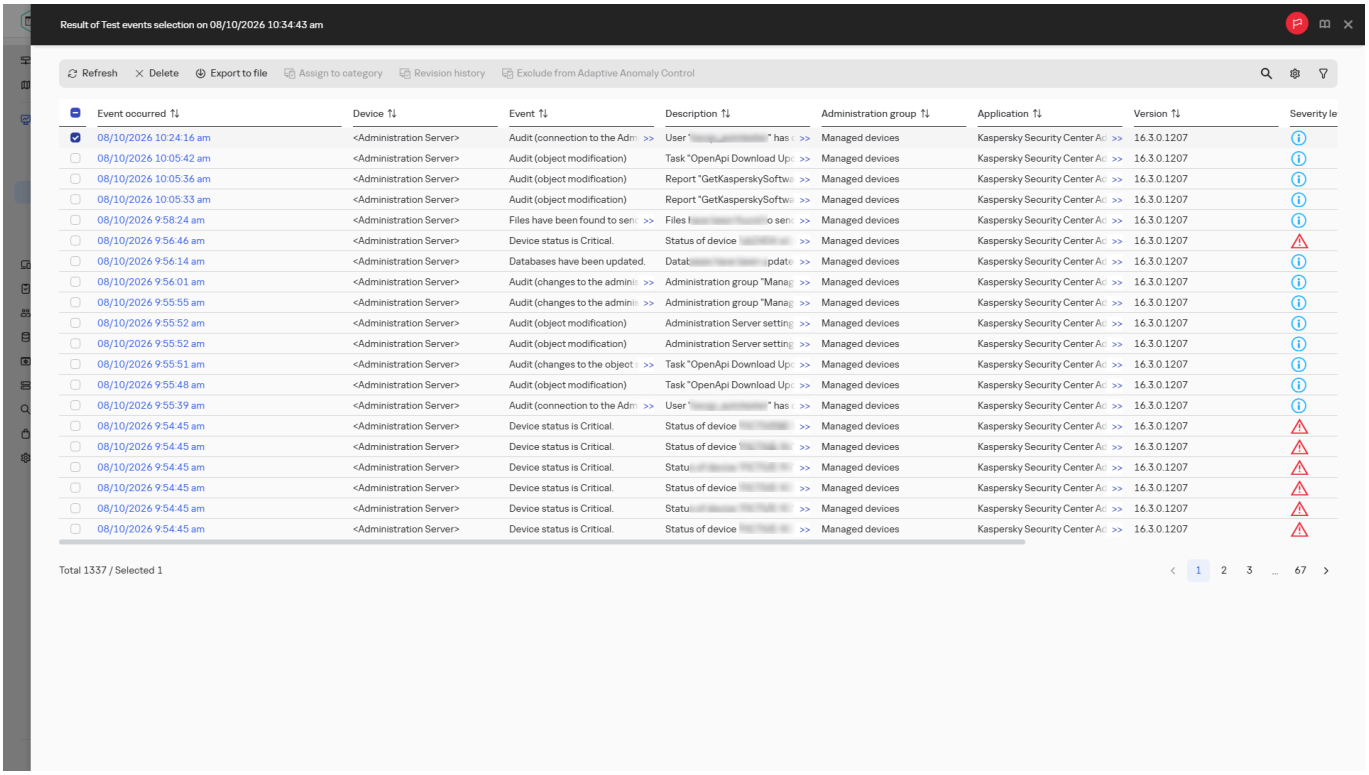
Kaspersky Security Center Linux позволяет сохранять события в файл формата CSV или TXT.

Чтобы экспортировать события из выборки событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Выборки событий**.
2. Нажмите на имя требуемой выборки.

3. Выберите события:

- Если вы хотите экспортировать одно или несколько событий, установите флажки рядом с ними.
- Если вы хотите экспортировать все события на текущей странице, установите флажок над списком событий и нажмите **Выбрать все на текущей странице**.
- Если вы хотите экспортировать все события из выборки, установите флажок над списком событий и нажмите **Выбрать все**.



Результат выборки событий

4. Нажмите на кнопку **Экспорт** и выберите **Экспортировать в CSV** или **Экспортировать в TXT**.

Чтобы экспортировать события из списка событий на устройстве:

1. Откройте список устройств.
   - Для управляемых устройств: **Управление активами** → **Управляемые устройства**.
   - Для нераспределенных устройств: **Управление активами** → **Нераспределенные устройства**.
2. В списке устройств нажмите на ссылку с названием нужного устройства и перейдите на вкладку **События**.

3. Выберите события:

   - Если вы хотите удалить одно или несколько событий, установите рядом с ними флажки.
   - Если вы хотите удалить все события на текущей странице, установите флажок над списком событий и выберите параметр **Выбрать все на текущей странице**.
   - Если вы хотите удалить все события из выборки, установите флажок над списком событий и выберите параметр **Выбрать все**.

4. Нажмите на кнопку **Экспорт** и выберите **Экспортировать в CSV** или **Экспортировать в TXT**.

Вся информация о выбранных событиях, включенных в таблицу, будет экспортирована.

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 события из выборки событий:

1. Запустите выборку событий.
2. Выберите события:

   - Если вы хотите удалить одно или несколько событий, установите рядом с ними флажки.
   - Если вы хотите удалить все события на текущей странице, установите флажок над списком событий и выберите параметр **Выбрать все на текущей странице**.
   - Если вы хотите удалить все события из выборки, установите флажок над списком событий и выберите параметр **Выбрать все**.

3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **Удалить**.

Чтобы удалить события из списка событий устройства:

1. Откройте список устройств.
   - Для управляемых устройств: **Управление активами** → **Управляемые устройства**.
   - Для нераспределенных устройств: **Управление активами** → **Нераспределенные устройства**.
2. В списке устройств нажмите на ссылку с названием нужного устройства и перейдите на вкладку **События**.
3. Выберите события:
   - Если вы хотите удалить одно или несколько событий, установите рядом с ними флажки.
   - Если вы хотите удалить все события на текущей странице, установите флажок над списком событий и выберите параметр **Выбрать все на текущей странице**.
   - Если вы хотите удалить все события из выборки, установите флажок над списком событий и выберите параметр **Выбрать все**.
4. Нажмите **Удалить** и подтвердите действие.
5. В появившемся окне нажмите на кнопку **Удалить**.

Выбранные события удалены и не могут быть восстановлены.

Удаление выборок событий

Можно удалять только пользовательские выборки событий. Предопределенные выборки событий невозможно удалить.

Чтобы удалить выборки событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Выборки событий**.
2. Установите флажки напротив выборок событий, которые требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **ОК**.

Выборка событий будет удалена.

Настройка срока хранения события

Kaspersky Security Center Linux позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования. Возможно, вам нужно хранить некоторые события в течение более длительного или более короткого периода, чем указано по умолчанию. Вы можете изменить срок хранения события по умолчанию.

Если вас не интересует сохранение каких-либо событий в базе данных Сервера администрирования, вы можете выключить соответствующий параметр в политике Сервера администрирования, политике приложения "Лаборатории Касперского" или в свойствах Сервера администрирования (только для событий Сервера администрирования). Это уменьшит количество типов событий в базе данных.

Чем больше срок хранения события, тем быстрее база данных достигает максимального размера. Однако более длительный срок хранения события позволяет выполнять задачи мониторинга и просматривать отчеты в течение более длительного периода.

Чтобы задать срок хранения события в базе данных Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на название требуемой политики.

   Вы можете выбрать политику управляемого приложения "Лаборатории Касперского", Агента администрирования или Сервера администрирования. Для Сервера администрирования вы можете настроить срок хранения событий, нажав на имя Сервера администрирования.
3. Выберите вкладку **Настройка событий**.

   Отображается раздел **Критическое** со списком связанных событий. При необходимости вы можете перейти в раздел **Отказ функционирования**, **Предупреждение** или **Информационное сообщение**.
4. 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 переключатель **Хранить в базе данных Сервера администрирования в течение (сут)**.
5. В поле редактирования под переключателем укажите количество дней для сохранения события.
6. 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, вы не сможете изменить значение срока хранения события.
7. Нажмите на кнопку **OK**, а затем после того, как правая панель закроется, нажмите на кнопку **Сохранить**.

   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

Управляемое приложение, например Kaspersky Endpoint Security для Linux, установленное на одном или нескольких управляемых устройствах, может отправлять на Сервер администрирования множество однотипных событий. Прием частых событий может привести к перегрузке базы данных Сервера администрирования и перезаписи других событий. Сервер администрирования начинает блокировать наиболее частые события, когда количество всех полученных событий превышает установленное ограничение для базы данных.

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 окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Блокировка частых событий**.

3. В разделе **Блокировка частых событий**:

   - Если вы хотите разблокировать прием частых событий:

     a. Выберите частые события, который нужно разблокировать, и нажмите на кнопку **Исключить**.

     b. Нажмите на кнопку **Сохранить**.

   - Если вы хотите заблокировать прием частых событий:

     a. Выберите частые события, которые вы хотите заблокировать и нажмите на кнопку **Заблокировать**.

     b. Нажмите на кнопку **Сохранить**.

Сервер администрирования принимает разблокированные частые события и не принимает заблокированные частые события.

Отмена блокировки частых событий

Вы можете отменить блокировку частых событий и начать получение событий до тех пор, пока Сервер администрирования снова не заблокирует эти частые события.

Чтобы отменить блокировку частых событий:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Блокировка частых событий**.

3. В разделе **Блокировка частых событий** нажмите строку частого события, для которого вы хотите отменить блокировку.

4. Нажмите на кнопку **Отменить блокировку**.

Частое событие удаляется из списка частых событий. Сервер администрирования будет получать события этого типа.

Обработка и хранение событий на Сервере администрирования

Информация о событиях, возникших в работе приложения и управляемых устройств, сохраняется в базе данных Сервера администрирования. Каждое событие относится к определенному типу и уровню важности (*Критическое событие*, *Отказ функционирования*, *Предупреждение*, *Информационное сообщение*). В зависимости от условий, при которых произошло событие, приложение может присваивать событиям одного типа разные уровни важности.

Вы можете просматривать типы и уровни важности событий в разделе **Настройка событий** окна свойств Сервера администрирования. В разделе **Настройка событий** вы также можете настроить параметры обработки каждого события Сервером администрирования:

- регистрацию событий на Сервере администрирования и в журналах событий операционной системы на устройстве и на Сервере администрирования;
- способ уведомления администратора о событии (например, SMS, сообщение электронной почты).

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, приложение вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400 000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Приложение проверяет базу данных каждые 10 минут. Если количество событий достигает на 10 000 больше указанного максимального значения, приложение удаляет самые старые события, чтобы осталось только указанное максимальное количество событий.

Когда Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий операционной системы. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления. 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.

Об уведомлениях

Уведомления информируют вас о важных событиях и помогают быстро отреагировать на них, выполнив рекомендуемые действия или другие соответствующие действия.

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 доступны в раскрывающейся панели, которая открывается при нажатии на значок уведомлений ( ), и в Центре уведомлений. Им присваивается один из следующих уровней важности: **Критическая**, **Предупреждение**, **Информационное сообщение** и **Успешно**.

Красная точка на значке означает, что есть непрочитанные уведомления.

Экранные уведомления сгруппированы по следующим типам:

- **Требуется внимание**

  Уведомления, требующие вашего внимания. Уведомления с уровнем важности **Критический** отображаются на главной информационной панели в дополнение к Центру уведомлений.

- **Система**

  Системные уведомления. Они разделены на следующие категории:

  - **Развертывание**
  - **Устройства**
  - **Защита**
  - **Обновления** (включая уведомления о доступных для скачивания приложений "Лаборатории Касперского", уведомления о скачанных обновлениях антивирусных баз и уведомления об устройствах, требующих перезагрузки после обновления Агента администрирования)
  - **Защита от эксплойтов**
  - **Сервер администрирования** (включает только события, связанные с Сервером администрирования)

- **Объявления**

  Уведомления, содержащие информацию о вашей версии Kaspersky Security Center Linux и управляемых приложениях, установленных на управляемых устройствах.

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 уведомлений, требующих внимания

Уведомления, требующие внимания, информируют вас о событиях, которые могут потребовать вашего участия. Им присваивается один из следующих уровней важности: **Критическая**, **Предупреждение**, **Информационное сообщение** и **Успешно**.

Уведомления с уровнем важности **Критическая** отображаются в Web Console в дополнении к уведомлениям из Центра уведомлений. Если есть несколько критичных уведомлений, Web Console отображает одно уведомление, показывающее общее количество предельных уведомлений.

Вы можете просмотреть уведомления, требующие внимания, одним из следующих способов:

- В раскрывающейся панели.

  В раскрывающейся панели отображаются только непрочитанные уведомления, требующие внимания. Если нет непрочитанных уведомлений, требующих внимания, вкладка **Требуется внимание** не отображается.

- В Центре уведомлений.

  Центр уведомлений отображает все уведомления, требующие внимания, включая прочитанные и непрочитанные уведомления. Если нет уведомлений, требующих внимания, вкладка **Требуется внимание** не отображается.

Чтобы просмотреть уведомления, требующие внимания, в раскрывающейся панели:

1. В верхней части окна приложения Web Console нажмите на значок уведомления ( ).

   Откроется панель **Уведомления**.

2. На вкладке **Требуется внимание** просмотрите непрочитанные уведомления.

3. При необходимости отметьте требуемые уведомления как прочитанные одним из следующих способов:

   - Чтобы отметить уведомление как прочитанное, нажмите на значок закрытия (×) рядом с уведомлением.

   - Чтобы отметить все объявления как прочитанные, нажмите на кнопку **Отметить как прочитанное**.

   После просмотра и отметки уведомлений, требующих внимания, вкладка **Требуется внимание** больше не отображается в раскрывающейся панели **Уведомления**. Вы можете просмотреть все уведомления, требующие внимания, в Центре уведомлений.

Чтобы просмотреть уведомления, требующие внимания, в Центре уведомлений:

1. В верхней части окна приложения Web Console нажмите на значок уведомления ( ).

2. В открывшейся панели **Уведомления** нажмите на кнопку **Перейти в Центр уведомлений**.

   Откроется окно **Центр уведомлений**.

3. На вкладке **Требуется внимание** выберите один из следующих разделов:

   - **Все уведомления, требующие внимания** – отображаются все уведомления, требующие внимания, независимо от их уровня важности.
   - **Критическая** – отображаются уведомления с уровнем важности **Критическая**.
   - **Предупреждение** – отображаются уведомления с уровнем важности **Предупреждение**.
   - **Информационное сообщение** – отображаются уведомления с уровнем важности **Информационное сообщение**.

4. Чтобы отображать только непрочитанные уведомления, включите переключатель **Показать только непрочитанное**.

5. В списке уведомлений нажмите на уведомление, чтобы просмотреть его текст. Полный текст уведомления отображается в панели сведений справа.

   Когда вы просматриваете уведомление, оно автоматически отмечается как прочитанное.

6. Чтобы отметить уведомления как прочитанные вручную, выполните одно из следующих действий:

   - Чтобы отметить уведомление как прочитанное, выберите его в списке уведомлений и нажмите на кнопку **Отметить как прочитанное**.
   - Чтобы отметить все уведомления как прочитанные, нажмите на кнопку **Отметить как прочитанное**.

7. При необходимости вы можете отметить уведомление как непрочитанное, выбрав его в списке уведомлений и нажав на кнопку **Отметить как непрочитанное**.

Уведомления, требующие внимания, просмотрены.

Просмотр системных уведомлений

Системные уведомления информируют вас о событиях, связанных с Web Console и с управляемыми устройствами. Системные уведомления сгруппированы по типам и имеют один из следующих уровней важности: **Критическая**, **Предупреждение**, **Информационное сообщение** и **Успешно**.

Вы можете просмотреть системные уведомления одним из следующих способов:

- В раскрывающейся панели.
- В Центре уведомлений.

Чтобы просмотреть системные уведомления, в раскрывающейся панели:

1. В верхней части окна приложения Web Console нажмите на значок уведомления ( ).

   Откроется панель **Уведомления**.

2. На вкладке **Система** просмотрите непрочитанные уведомления.

3. При необходимости отметьте системные уведомления как прочитанные одним из следующих способов:

   - Чтобы отметить уведомление как прочитанное, нажмите на значок закрытия (×) рядом с уведомлением.

   - Чтобы отметить все объявления как прочитанные, нажмите на кнопку **Отметить как прочитанное**.

   После того как вы просмотрите все системные уведомления и отметите их как прочитанные, в раскрывающейся панели **Уведомления** отобразится сообщение об отсутствии новых уведомлений. Вы можете просмотреть все системные уведомления, прочитанные и непрочитанные, в Центре уведомлений.

Чтобы просмотреть системные уведомления в Центре уведомлений:

1. В верхней части окна приложения Web Console нажмите на значок уведомления ().

2. В открывшейся панели **Уведомления** нажмите на кнопку **Перейти в Центр уведомлений**.

   Откроется окно **Центр уведомлений**.

3. На вкладке **Система** выберите один из следующих разделов:

   - **Все системные уведомления**
   - **Развертывание**
   - **Устройства**
   - **Защита**
   - **Обновления**
   - **Защита от эксплойтов**
   - **Сервер администрирования**

4. Чтобы отображать только непрочитанные уведомления, включите переключатель **Показать только непрочитанное**.

5. В списке уведомлений нажмите на уведомление, чтобы просмотреть его текст. Полный текст уведомления отображается в панели сведений справа.

   Когда вы просматриваете уведомление, оно автоматически отмечается как прочитанное.

6. Чтобы отметить уведомления как прочитанные вручную, выполните одно из следующих действий:

   - Чтобы отметить уведомление как прочитанное, выберите его в списке уведомлений и нажмите на кнопку **Отметить как прочитанное**.

   - Чтобы отметить все уведомления как прочитанные, нажмите на кнопку **Отметить как прочитанное**.

7. При необходимости вы можете отметить уведомление как непрочитанное, выбрав его в списке уведомлений и нажав на кнопку **Отметить как непрочитанное**.

Системные уведомления просмотрены.

Просмотр объявлений

Объявления – это тип уведомлений, которые содержат информацию о вашей версии Kaspersky Security Center Linux и версиях приложений "Лаборатории Касперского", установленных на ваших управляемых устройствах. Отображаются только объявления, относящиеся к текущему подключенному Серверу администрирования и приложениям "Лаборатории Касперского", установленным на управляемых устройствах этого Сервера администрирования. Объявления отображаются отдельно для каждого Сервера администрирования, главного, подчиненного или виртуального.

Если несколько администраторов используют Kaspersky Security Center Linux и устанавливают разные языки интерфейса, Kaspersky Security Center Linux отображает объявления "Лаборатории Касперского" на всех языках, используемых администраторами. При изменении языка интерфейса объявления "Лаборатории Касперского" на выбранном языке автоматически добавляются в раздел после выхода из Web Console и повторного входа.

Объявления включают следующие типы информации:

- Информация, связанная с безопасностью.

  Объявления, связанные с безопасностью, включают критические обновления, исправления для уязвимостей и рекомендации по устранению проблем в приложениях "Лаборатории Касперского". Объявления, связанные с безопасностью, включены по умолчанию. Если вы не хотите получать объявления, связанные с безопасностью, вы можете выключить эту функцию.

  Вы не можете отключить объявления, связанные с безопасностью, в пробном режиме Kaspersky Security Center Linux.

  Для предоставления информации, которая соответствует вашей конфигурации защиты сети, Kaspersky Security Center Linux отправляет данные на облачные серверы "Лаборатории Касперского" и получает только те объявления, которые относятся к приложениям "Лаборатории Касперского", установленным в вашей сети. Данные, которые могут быть отправлены на серверы, описаны в Лицензионном соглашении, которое вы принимаете при создании рабочей области Kaspersky Security Center Linux.

- Маркетинговая информация.

  Маркетинговая объявления включают специальные предложения, новости о приложениях и рекламу приложений "Лаборатории Касперского". Маркетинговые объявления доступны, только если включен Kaspersky Security Network (KSN). Вы можете выключить маркетинговые объявления, выключив KSN.

  Чтобы предоставить информацию, которая может помочь вам защитить ваши сетевые устройства и выполнять повседневные задачи, Kaspersky Security Center Linux 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.

Объявлениям присваивается один из следующих уровней важности: **Критическая**, **Предупреждение**, **Информационное сообщение** и **Успешно**.

Вы можете просмотреть объявления одним из следующих способов:

- В раскрывающейся панели.
- В Центре уведомлений.

Чтобы просмотреть объявления в раскрывающейся панели:

1. В верхней части окна приложения Web Console нажмите на значок уведомления ( ).

   Откроется панель **Уведомления**.

2. На вкладке **Объявления** просмотрите непрочитанные уведомления.

3. При необходимости отметьте объявления как прочитанные одним из следующих способов:

   - Чтобы отметить уведомление как прочитанное, нажмите на значок закрытия (×) рядом с уведомлением.
   - Чтобы отметить все объявления как прочитанные, нажмите на кнопку **Отметить как прочитанное**.

После того как вы просмотрите все уведомления и отметите их как прочитанные, в раскрывающейся панели **Уведомления** отобразится сообщение об отсутствии новых уведомлений. Вы можете просмотреть все объявления, прочитанные и непрочитанные, в Центре уведомлений.

Чтобы просмотреть объявления в Центре уведомлений:

1. В верхней части окна приложения Web Console нажмите на значок уведомления ( ).

2. В открывшейся панели **Уведомления** нажмите на кнопку **Перейти в Центр уведомлений**.

   Откроется окно **Центр уведомлений**.

3. На вкладке **Объявления** выберите один из следующих разделов:

   - **Все объявления** – отображаются все уведомления, независимо от их уровня важности.
   - **Критическая** – отображаются уведомления с уровнем важности **Критическая**.
   - **Предупреждение** – отображаются уведомления с уровнем важности **Предупреждение**.
   - **Информационное сообщение** – отображаются уведомления с уровнем важности **Информационное сообщение**.

4. Чтобы отображать только непрочитанные уведомления, включите переключатель **Показать только непрочитанное**.

5. В списке уведомлений нажмите на уведомление, чтобы просмотреть его текст. Полный текст уведомления отображается в панели сведений справа.

   Когда вы просматриваете уведомление, оно автоматически отмечается как прочитанное.

6. Чтобы отметить уведомления как прочитанные вручную, выполните одно из следующих действий:

   - Чтобы отметить уведомление как прочитанное, выберите его в списке уведомлений и нажмите на кнопку **Отметить как прочитанное**.
   - Чтобы отметить все уведомления как прочитанные, нажмите на кнопку **Отметить как прочитанное**.

7. При необходимости вы можете отметить уведомление как непрочитанное, выбрав его в списке уведомлений и нажав на кнопку **Отметить как непрочитанное**.

Объявления просмотрены.

Выключение объявлений "Лаборатории Касперского"

Раздел объявлений "Лаборатории Касперского" (**Мониторинг → Объявления "Лаборатории Касперского"**) предоставляет информацию о вашей версии Kaspersky Security Center Linux и управляемых приложениях, установленных на управляемых устройствах. Если вы не хотите получать объявления "Лаборатории Касперского", вы можете отключить эту функцию.

Объявления "Лаборатории Касперского" включают в себя информацию двух типов: объявления, связанные с безопасностью, и рекламные объявления.

Чтобы выключить объявления, связанные с безопасностью:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Объявления "Лаборатории Касперского"**.

3. Переведите переключатель в положение **Объявления, связанные с безопасностью**, выключено.

4. Нажмите на кнопку **Сохранить**.

   Объявления "Лаборатории Касперского" выключены.

Рекламные объявления по умолчанию выключены. Вы получаете рекламные сообщения только в том случае, если вы включили Kaspersky Security Network (KSN). Вы можете выключить этот тип объявлений, отключив KSN.

Отключение KSN может повлиять на работу управляемых приложений "Лаборатории Касперского", использующих службы KSN. Эти приложения могут утратить возможность обмена данными о репутации, телеметрией или статистикой с "Лабораторией Касперского".

Настройка переключения статусов устройств

Вы можете изменить условия присвоения статусов *Критический* или *Предупреждение* устройству.

Чтобы изменить статус устройства на Критический:

1. В главном окне приложения перейдите в раздел **Управление активами → Иерархия групп**.

2. Перейдите в свойства группы администрирования, для которой вы хотите изменить статусы устройств, одним из следующих способов:

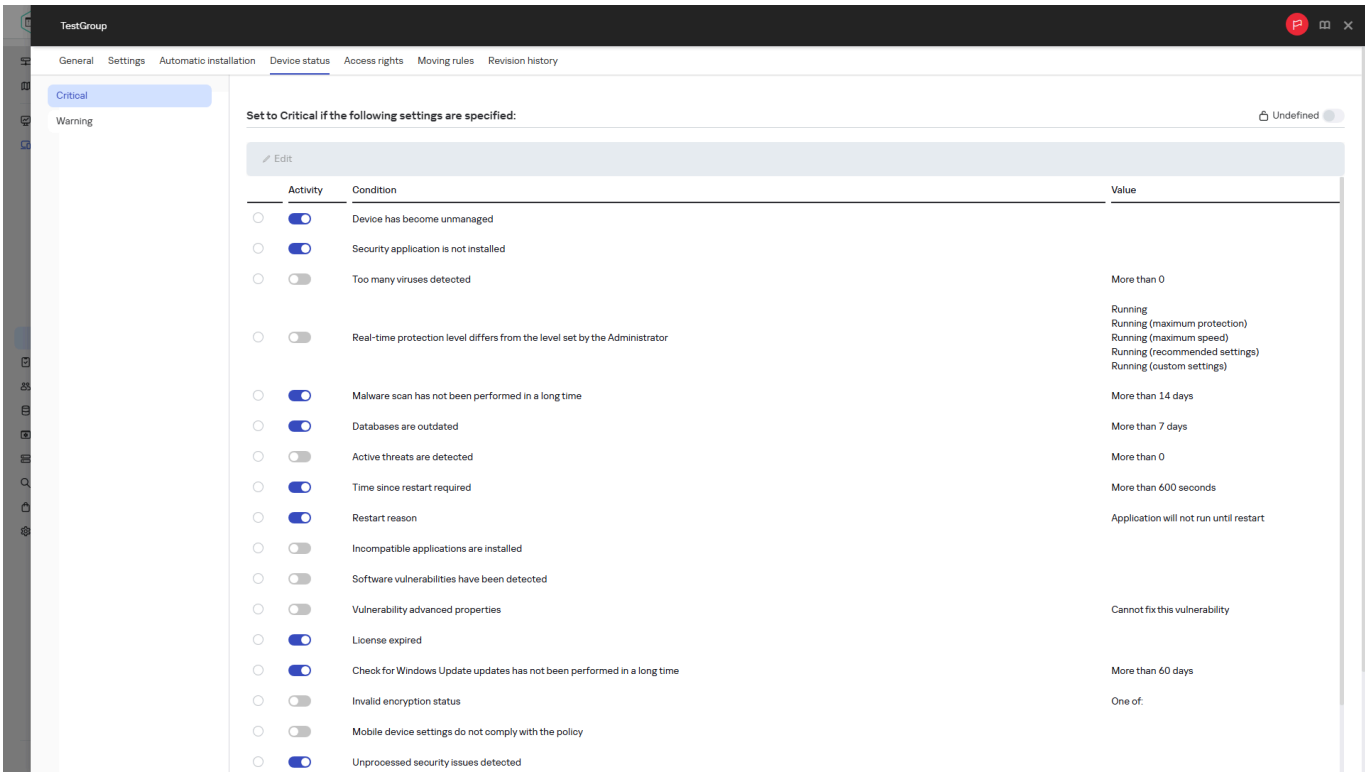
   - Выберите имя группы администрирования.
   - Нажмите на кнопку **Показать иерархию** в верхней части страницы. В открывшейся панели наведите курсор мыши на название нужной группы и нажмите на значок параметров (⚙).

   Откроется окно свойств группы администрирования.

3. В окне свойств выберите вкладку **Статус устройства**.

4. Выберите раздел **Критический**.

5. В блоке **Установить статус "Критический", если** включите условие, чтобы перевести устройство в состояние *Критическое*.



> Вы можете изменить только 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**.

10. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

При выполнении заданных условий управляемому устройству присваивается статус *Критический*.

Чтобы изменить статус устройства на Предупреждение:

1. В главном окне приложения перейдите в раздел **Управление активами → 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 вкладку **Статус устройства**.

4. Выберите раздел **Предупреждение**.

5. В блоке **Установить статус "Предупреждение", если**, включите условие, чтобы переключить устройство в состояние *Предупреждение*.

   Вы можете изменить только 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**.
10. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

При выполнении заданных условий управляемому устройству присваивается статус *Предупреждение*.

Настройка параметров доставки уведомлений

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 приложение Kaspersky Security Center Linux посылает уведомление на указанные адреса электронной почты.
- SMS – при возникновении события приложение 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 окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Перейдите в раздел **Уведомление** и на правой панели выберите вкладку с требуемым способом уведомления:

   - **Электронная почта**

     На вкладке **Электронная почта** можно настроить уведомления о событиях по электронной почте.

     В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

     - IPv4-адрес или IPv6-адрес;
     - DNS-имя SMTP-сервера.

     В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Если вы включите параметр **Использовать DNS и MX поиск**, вы сможете использовать несколько MX-записей IP-адреса для одного и того же DNS-имени SMTP-сервера. Одно DNS-имя может иметь несколько MX-записей с различными приоритетами полученных электронных писем. Сервер администрирования пытается отправлять уведомления по электронной почте на SMTP-сервер в порядке возрастания приоритета MX-записей.

Если вы включили параметр **Использовать DNS и MX поиск** и не разрешили использование параметров TLS, рекомендуется использовать параметры DNSSEC на вашем серверном устройстве в качестве дополнительной меры защиты при отправке уведомлений по электронной почте.

Если параметр **Использовать ESMTP-аутентификацию** включен, вы можете указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию параметр не выбран и параметры ESMTP-аутентификации недоступны.

Вы можете указать параметры подключения TLS для SMTP-сервера:

- **Не использовать TLS**

Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

- **Использовать TLS, если поддерживается SMTP-сервером**

Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.

- **Всегда использовать TLS, 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 pkcs12:

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: приложение отправляет тестовые сообщения на указанные адреса электронной почты.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой.

В поле **Тема** укажите тему электронной почты, используя подстановочные параметры, например: `[KSC-SAMARA-1] [%SEVERITY%] %EVENT%`. Пример отображения темы письма в случае обнаружения угрозы: `[KSC-SAMARA-1] [Critical] Threat detected`. Также 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. Не рекомендуется указывать в этом поле несуществующий адрес электронной почты** укажите адрес отправителя электронной почты. Если вы оставите поле пустым, по умолчанию используется адрес получателя. Не рекомендуется использовать несуществующий адрес.

В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый приложением при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив подстановочные параметры с подробными данными события.

Пример заполнения поля

```
Sender - KSC-SAMARA-1

Host: %COMPUTER%

Product: %KL_PRODUCT%

Version: %KL_VERSION%

Occurred at: %RISE_TIME%

Event: %EVENT%

Details:

%DESCR%
```

Строка `Sender` является необязательной. Например, если у вас несколько Серверов администрирования, вы можете указать в качестве значения имя Сервера администрирования, с которого поступило уведомление: `Sender - KSC-SAMARA-1`.

Пример отображения текста уведомления:

```
Sender - KSC-SAMARA-1
```

```
Host: nb-123456.example.net

Product: Kaspersky Endpoint Security 12.5 for Linux

Version: 12.5.0.1569

Occurred at: 2026-08-17T13:15:36

Event: Threat detected

Details:

Initiator: Product; Task type: ODS; ID of running task: 107; User receiving access:
root; Object type: File; File owner: user; Detection certainty: Sure; File:
/home/user/eicar_com.zip//eicar.com; Detected object name: EICAR-Test-File; Detected
object type: Virware; MD5 hash: <hash>; Unique ID: <ID>
```

> Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

- **SMS**

На вкладке **SMS** можно настроить отправку SMS-уведомлений о различных событиях на мобильный телефон. SMS-сообщения отправляются через почтовый шлюз.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес;
- Имя устройства в сети Windows (NetBIOS-имя);
- DNS-имя SMTP-сервера.

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Если параметр **Использовать ESMTP-аутентификацию** включен, вы можете указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию параметр не выбран и параметры ESMTP-аутентификации недоступны.

Вы можете указать параметры подключения TLS для SMTP-сервера:

- **Не использовать TLS**

Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

- **Использовать TLS, если поддерживается SMTP-сервером**

Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.

- **Всегда использовать TLS, для проверки срока действия сертификата сервера**

Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы 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. Не рекомендуется указывать в этом поле несуществующий адрес электронной почты** укажите адрес отправителя электронной почты. Если вы оставите поле пустым, по умолчанию используется адрес получателя. Не рекомендуется использовать несуществующий адрес.

В поле **Номера телефонов получателей SMS-сообщений** укажите номера мобильных телефонов для получения SMS.

В поле **Текст уведомления** напишите текст уведомления о событии, отправляемый приложением при возникновении события. Текст может содержать подстановочные параметры, такие как имя события, имя устройства и имя домена.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

Нажмите на кнопку **Отправить тестовое сообщение**, чтобы проверить правильно ли настроены сообщения: приложение отправляет тестовые сообщения указанным получателям.

- **Исполняемый файл для запуска**

  Исполняемый файл должен содержать переменные среды события, которые нужно передать администратору.

  В поле **Исполняемый файл, который запустится на Сервере администрирования при возникновении события** укажите папку и имя файла, который запустится.

  Пример заполнения поля:

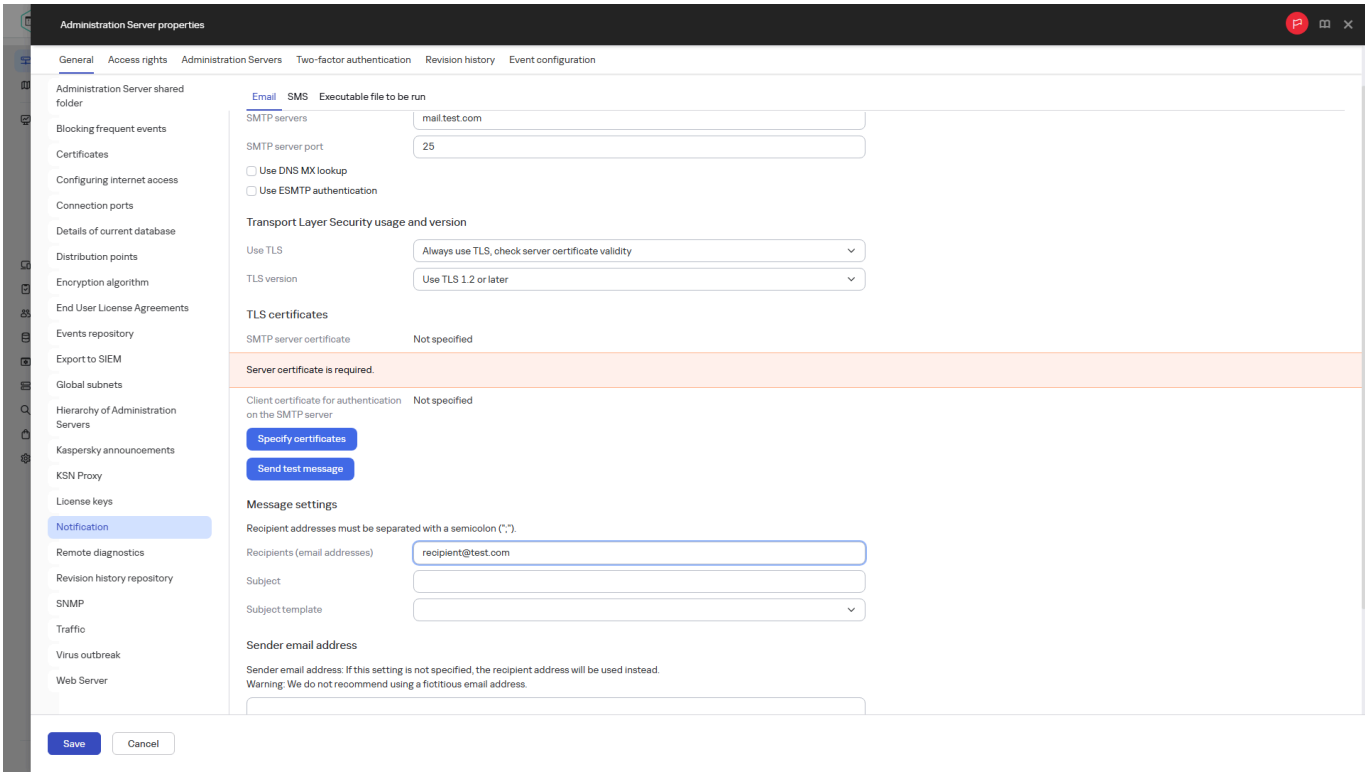
```
/opt/scripts/notifications.sh
```

Файл необходимо подготовить заранее, указав в нем подстановочные параметры, определяющие сведения о событии, которые будут отправлены в сообщении. Папка и файл должны находиться на Сервере администрирования.

Пример скрипта для тестов или отладки:

```
#!/usr/bin/env bash
touch /tmp/ksc_notification.txt
echo "$RISE_TIME $COMPUTER $EVENT" >> /tmp/ksc_notification.txt
```

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.



Выбор способа уведомления

3. На вкладке настройте параметры уведомлений.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения и 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 приложения.

Проверка распространения уведомлений

Для проверки распространения уведомлений о событиях используется уведомление об обнаружении тестового "вируса" Eicar на клиентских устройствах.

Чтобы проверить распространение уведомлений о событиях:

1. Остановите задачу постоянной защиты файловой системы на клиентском устройстве и скопируйте тестовый "вирус" Eicar на клиентское устройство. Затем снова включите задачу постоянной защиты файловой системы.

2. Запустите задачу проверки клиентских устройств для группы администрирования или набора устройств, в который входит клиентское устройство с тестовым "вирусом" Eicar.

   Если задача проверки настроена верно, в процессе ее выполнения тестовый "вирус" будет обнаружен. Если параметры уведомлений настроены верно, вы получите уведомление о найденном вирусе.

Чтобы открыть запись об обнаружении тестового "вируса":

1. В главном окне приложения перейдите в раздел **Мониторинг → Выборки событий**.

2. Нажмите на название выборки **Последние события**.

   В открывшемся окне отображается уведомление о тестовом "вирусе".

Тестовый "вирус" Eicar не содержит программного кода, который может навредить вашему устройству. При этом большинство приложений безопасности компаний-производителей идентифицируют его как вирус. Загрузить тестовый "вирус" можно с официального веб-сайта организации EICAR.

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). 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*. 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*.
- *OK* или *OK/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
Приложение безопасности не установлено	Агент администрирования установлен на устройстве, но не установлено приложение безопасности.	• Переключатель включен. • Переключатель выключен.

Условие	Описание условия	Доступные значения
Обнаружено много вирусов	В результате работы задач поиска вирусов, например, задачи Поиск вредоносного ПО, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение.	Более 0.
Уровень постоянной защиты отличается от уровня, установленного администратором	Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства.	• Остановлена. • Приостановлена. • Выполняется.
Давно не выполнялся поиск вредоносного ПО	Устройство видимо в сети и на устройстве установлено приложение безопасности, но ни задача *Поиск вредоносного ПО*, ни задача локальной проверки не выполнялись больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее.	Более 1 дня.
Базы устарели	Устройство видимо в сети и на устройстве установлено приложение безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее.	Более 1 дня.
Давно не 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.
Время, прошедшее с момента перезапуска	Устройство видимо в сети, но перезапуск требуется приложением уже дольше указанного интервала времени.	Более чем 0 минут.
Причина перезапуска	Устройство видимо в сети, но приложению требуется перезагрузка устройства по одной из выбранных причин.	• Неизвестная причина • Приложение неработоспособно до перезагрузки • Для завершения обновления требуется перезагрузка; приложение работоспособно • Для инициации обновления требуется перезагрузка • Для завершения проверки или лечения требуется перезагрузка • Требуется перезагрузка для завершения удаленной установки или удаления • Завершение шифрования данных на диске
Установлены несовместимые приложения	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые приложения.	• Переключатель выключен. • Переключатель включен.
Обнаружены уязвимости в приложениях	Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи *Поиск уязвимостей и требуемых обновлений* на устройстве обнаружены уязвимости в приложениях с заданным уровнем критичности.	• Предельный. • Высокий. • Средний. • Игнорировать, если невозможно закрыть уязвимость. • Игнорировать, если обновление назначено к установке.
Срок действия лицензии истек	Устройство видимо в сети, но срок действия лицензии истек.	• Переключатель выключен. • Переключатель включен.
Срок действия лицензии скоро истекает	Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.	Более чем 0 дней.

Условие	Описание условия	Доступные значения
Давно не выполнялась проверка обновлений Центра обновления Windows	Устройство видимо в сети, но задача *Поиск уязвимостей и требуемых обновлений* не выполнялась больше указанного времени.	Более 1 дня.
Недопустимый статус шифрования	Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению.	• Не соответствует политике из-за отказа пользователя (только для внешних устройств). • Не соответствует политике из-за ошибки. • В процессе применения политики – требуется перезагрузка. • Не задана политика шифрования. • Не поддерживается. • В процессе применения политики.
Параметры мобильного устройства не соответствуют политике	Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия.	• Переключатель выключен. • Переключатель включен.
Есть необработанные проблемы безопасности	На устройстве есть необработанные проблемы безопасности. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором.	• Переключатель выключен. • Переключатель включен.
Статус устройства определен приложением	Статус устройства определяется управляемым приложением. Управляемые устройства могут иметь статус, определяемый управляемыми приложениями, независимо от параметров Kaspersky Security Center Linux. После того как этот статус вернет один из статусов, определенных Kaspersky Security Center Linux, Сервер администрирования Kaspersky Security Center присваивает управляемому устройству предельный статус из тех, которые были возвращены управляемым приложением и присвоены Сервером администрирования Kaspersky Security Center. Статусы устройств определенные приложениями имеют описания, переданные управляемыми приложениями. Вы можете просмотреть описания в списке управляемых устройств в столбце **Описание статуса**.	• Переключатель выключен. • Переключатель включен.
На устройстве заканчивается дисковое пространство	Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы *Критический* или *Предупреждение* меняются на статус *ОК*, когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению.	Более чем 0 МБ.
Устройство стало неуправляемым	Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования.	• Переключатель выключен. • Переключатель включен.
Защита выключена	Устройство видимо в сети, но приложение безопасности на устройстве отключено больше указанного времени. В этом случае состояние приложения безопасности *Остановлено* или *Сбой* и отличается от следующих: *Запускается*, *Выполняется* или *Приостановлена*.	Более чем 0 минут.
Приложение безопасности не запущено	Устройство видимо в сети и приложение безопасности установлено на устройстве, но не запущено.	• 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 *ОК*.

Разным значениям одного условия могут соответствовать разные статусы. Например, по умолчанию при соблюдении условия **Базы устарели** со значением **Более 3** дней клиентскому устройству присваивается статус *Предупреждение*, а со значением **Более 7 дней** – статус *Критический*.

Если вы обновляете Kaspersky Security Center Linux с предыдущей версии, значение условия **Базы устарели** для назначения статуса *Критический* или *Предупреждение* не изменится.

Параметры и переменные среды для описания события

При настройке уведомлений о событиях, возникающих в Kaspersky Security Center Linux, вы можете использовать для их описания параметры и переменные среды (см. таблицу ниже).

Если в качестве способа уведомления вы выбрали запуск исполняемого файла, используйте переменные при написании файла.

Если вы хотите отправлять уведомления о событиях по электронной почте или SMS, при настройке уведомлений на соответствующей вкладке вы также можете указать переменные в полях **Тема** и **Текст уведомления**.

Параметры и переменные среды для описания события

Параметр подстановки (для использования в уведомлениях)	Переменная среды (для использования в скриптах)	Описание переменной среды
%SEVERITY%	$SEVERITY	Уровень важности события. Возможные значения: • **Информационное сообщение** • **Предупреждение** • **Сбой** • **Критическое**
%COMPUTER%	$COMPUTER	Имя устройства, на котором произошло событие. Максимальная длина имени устройства равна 256 символов.
%DOMAIN%	$DOMAIN	Имя домена устройства, на котором произошло событие.
%EVENT%	$EVENT	Имя типа события. Максимальная длина названия типа события равна 50 символов.
%DESCR%	$DESCR	Описание события. Максимальная длина описания равна 1000 символов.
%RISE_TIME%	$RISE_TIME	Время создания события.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	$KLCSAK_EVENT_TASK_DISPLAY_NAME	Название задачи. Максимальная длина названия задачи равна 100 символов.
%KL_PRODUCT%	$KL_PRODUCT	Название приложения.
%KL_VERSION%	$KL_VERSION	Номер версии приложения.
%$KLCSAK_EVENT_SEVERITY_NUM%	$KLCSAK_EVENT_SEVERITY_NUM	Код уровня важности события. Возможные значения: • 1 – **Информационное сообщение**. • 2 – **Предупреждение**. • 3 – **Сбой**. • 4 – **Критическое**.

Параметр подстановки (для использования в уведомлениях)	Переменная среды (для использования в скриптах)	Описание переменной среды
%HOST_IP%	$HOST_IP	IP-адрес устройства, на котором произошло событие.
%HOST_CONN_IP%	$HOST_CONN_IP	IP-адрес соединения устройства, на котором произошло событие.

Просмотр информации об обнаруженных угрозах

Вы можете включить или отключить отображение информации об алертах.

После активации Сервера администрирования по лицензии Kaspersky Extended Detection and Response Optimum или по лицензии Kaspersky Security для бизнеса Профессиональный, Kaspersky Security Center Web Console автоматически отображает подраздел **Алерты** в разделе **Мониторинг** в главном меню приложения.

*Чтобы включить или выключить отображение раздела **Алерты** в главном меню:*

1. В главном окне приложения перейдите в раздел **Параметры → Параметры интерфейса**.
2. Включите или выключите параметр **Показать EDR-алерты**.
3. Нажмите на кнопку **Сохранить**.

Если параметр включен **Показать EDR-алерты**, в консоли отображается раздел **Алерты** в разделе **Мониторинг** главного меню. В разделе **Алерты** вы можете просматривать информацию об обнаруженных угрозах на устройствах.

Также вы можете добавить виджет, в котором отображается информация об алертах.

Для корректного отображения подробной информации об обнаруженных угрозах в карточке алерта вам необходимо установить плагин Kaspersky Endpoint Agent и совместимую версию плагина Kaspersky Endpoint Security (Kaspersky Endpoint Security для Linux 12.1 или выше, Kaspersky Endpoint Security для Mac 12.1 или выше, Kaspersky Endpoint Security для Windows 12.6 или выше).

Используйте меню **Фильтр**, чтобы отфильтровать алерты по дате и значениям поля.

Поле **Тип объекта** содержит одно из следующих значений:

- неизвестно
- Фишинговая ссылка
- вирус
- троянское приложение
- вредоносные утилиты
- троянское приложение удаленного администрирования
- червь
- другое приложение

- Рекламное приложение
- Порнографическое приложение
- Опасно упакованное приложение
- Опасное поведение

Поле **Автоматический ответ** содержит одно из следующих значений:

- Обнаружен вредоносный объект
- Объект удален
- Объект вылечен
- Не удалось вылечить объект
- Объект помещен на карантин
- Обнаружен архив, защищенный паролем
- Обнаружен вирус

Интеграции для реагирования на алерты

Если у вас есть лицензия Kaspersky Security для бизнеса Профессиональный, вы можете настроить интеграцию со следующими решениями для реагирования на угрозы:

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

Эти интеграции доступны, если вы активировали Сервер администрирования по лицензии Kaspersky Security для бизнеса Профессиональный.
Для выполнения действий по реагированию вам нужно распространить лицензионный ключ Kaspersky Security для бизнеса Профессиональный на управляемые приложения.
При использовании функциональности Kaspersky Security для бизнеса Профессиональный по пробной лицензии вам нужно сначала добавить физический подчиненный Сервер администрирования, активировать этот подчиненный Сервер администрирования по пробной лицензии и распространить лицензионный ключ на ваши устройства, управляемые этим Сервером администрирования.

Если у вас есть лицензии Kaspersky Next EDR Optimum, вам не нужно активировать приложения, установленные на ваших управляемых устройствах по лицензии Kaspersky Security для бизнеса Профессиональный. Вам нужно сделать это только для новых устройств (при их наличии).

Поскольку лицензия Kaspersky Security для бизнеса Профессиональный поддерживает мультитенантность, вы можете централизованно распространять лицензионный ключ на управляемые приложения. Автоматическое распространение лицензии на подчиненные и виртуальные Серверы администрирования не поддерживается.

Чтобы настроить интеграцию, у вас должны быть права **Чтение** и **Запись** для функциональной области **Общие функции: Интеграция приложения**.

Настройка интеграции с Active Directory для выполнения действий по реагированию

Интеграция с Active Directory позволяет выполнять действия по реагированию для пользователей Active Directory, затронутых или вовлеченных в алерт.

Чтобы настроить интеграцию с Active Directory для реагирования на алерты, вам нужно использовать Сервер администрирования Kaspersky Security Center Linux версии 15.4 или выше.

Интеграция с Active Directory для реагирования на алерты и параметры проверки контроллера домена Active Directory (адрес и учетные данные пользователя контроллера домена), который вы указываете при настройке опроса контроллера домена, это два разных параметра. Поскольку вам нужно убедиться, что у пользователя, для которого должно выполняться действие по реагированию, есть учетная запись Active Directory, требуется настроить обе интеграции: для проверки и для реагирования. Порядок не имеет значения.

Параметры интеграции не наследуются, а применяются только к Серверу администрирования (физическому или виртуальному), на котором вы настраиваете эти параметры.

Чтобы настроить интеграцию с Active Directory для реагирования на алерты:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Выполните одно из следующих действий:

   - Выберите раздел **Точки распространения**, нажмите на название нужной точки распространения и в открывшемся окне свойств выберите раздел **Active Directory**.
   - Выберите раздел **Реагирование через Active Directory**.

3. В правой панели включите переключатель **Интеграция с Active Directory**.

   Если вы захотите позже выключить интеграцию, вы можете сделать это только для всех соединений, выключив переключатель **Интеграция с Active Directory**. Выключить интеграцию для отдельного соединения невозможно. Вы можете удалить соединение.

   > Когда вы включаете или выключаете переключатель **Интеграция с Active Directory**, этот параметр применяется как для раздела **Реагирование через Active Directory** и для раздела **Точки распространения**.

4. Создайте соединение к контроллеру домена Active Directory, нажав на кнопку **Добавить**.

5. В открывшемся окне настройте следующие параметры для соединения:

   - **Адрес контроллера домена**

     Имя компьютера, например: `server.mycompany.com`.

     Вы можете указать несколько IP-адресов. Все контроллеры домена, IP-адреса которых вы указываете, должны принадлежать одному домену.

- **Имя домена Active Directory**

  Полное доменное имя DNS, например: `mycompany.com`.

  Также вы можете указать SAM-имя или NetBIOS-имя, например: `mycompany`.

  Используйте строчные буквы. Если вы создаете несколько соединений для Сервера администрирования или точки распространения, укажите разные имена для каждого соединения.

  > Для выполнения действий по реагированию имя домена Active Directory, указанное в этом поле, должно совпадать с именем домена Active Directory, указанным в алерте.

- **Учетная запись**

  Войдите в Active Directory под учетной записью с правами администратора, под которой будут выполняться действия по реагированию.

- **Пароль**

  Пароль учетной записи Active Directory с правами администратора, под которой будут выполняться действия по реагированию.

6. Если вы хотите проверить статус соединения, нажмите на кнопку **Проверить подключение**.

   Если соединение установлено, отображается статус **Подключено**. Иначе отображается статус **Сбой** и сообщение об ошибке с контроллерами домена, к которым не удалось подключиться.

> Вам нужно учитывать способ подключения к Active Directory: **с Linux-устройства или с Windows-устройства**

Подключение с Linux-устройства

По умолчанию при подключении и аутентификации к контроллеру домена с Linux-устройства используется следующая логика:

1. Сервер администрирования или точка распространения пытается подключиться к контроллеру домена через LDAPS.

   Выполняется строгая проверка сертификата LDAP-сервера.

2. Вы помещаете открытую часть сертификата контроллера домена в хранилище действительных сертификатов системы для проверки сертификата.

   Для доступа к цепочке сертификатов системы используется зависящий от операционной системы путь к центру сертификации (CA).

   Например:

   - /etc/ssl/certs/ca-certificates.crt – путь для операционных систем на базе Debian (Debian, Ubuntu, Astra).

   - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem – путь для CentOS или Red Hat.

3. Если не удается выполнить LDAPS-соединение, возникает ошибка и никакой другой протокол соединения использовать невозможно.

> В случае возникновения проблем с LDAPS вы можете обратиться в Службу технической поддержки "Лаборатории Касперского".

Если вы не хотите устанавливать сертификат в хранилище сертификатов системы, вы можете использовать флаг KLNAG_LDAP_SSL_CACERT, чтобы задать путь к сертификату контроллера домена. Для этого выполните команду:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

где `</path/to/domain-controller/cert>` – путь к открытой части сертификата контроллера домена.

Например, если путь равен `"/var/opt/kaspersky/ldap_cert.crt"`, команда будет иметь вид `klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

Подключение с Windows-устройства

При подключении и аутентификации к контроллеру домена с Windows-устройства параметры подключения определяются доменом.

Вам нужно только убедиться в следующем:

- LDAPS включен и порт 636 доступен на устройстве.
- Вы разрешаете подключения к контроллеру домена через сетевой экран или прокси-сервер.

7. Нажмите на кнопку **Сохранить**.

Окно закроется и соединение отобразится в списке соединений.

В таблице соединений можно выполнять следующие действия:

- Изменять параметры соединения.

  Для этого перейдите по ссылке с параметром **Адрес контроллера домена** для нужного соединения. В открывшемся окне измените нужные параметры и нажмите на кнопку **Сохранить**.

  Вы можете изменить только параметры **Учетная запись** и **Пароль**.

- Удалять подключения.

  Для этого установите флажок рядом с тем соединением, которое вы хотите удалить, в панели инструментов нажмите на кнопку **Удалить** и подтвердите удаление соединения.

Настройка интеграции с Kaspersky Automated Security Awareness Platform

Интеграция с Kaspersky Automated Security Awareness Platform (далее также KASAP) позволяет назначать учебные курсы KASAP для пользователей, связанных с алертами.

Параметры интеграции не наследуются, а применяются только к Серверу администрирования (физическому или виртуальному), на котором вы настраиваете эти параметры.

Перед настройкой интеграции в Kaspersky Security Center Web Console необходимо создать токен авторизации и получить URL для API-запросов в KASAP.

Чтобы настроить интеграцию с Kaspersky Automated Security Awareness Platform:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Выберите раздел **KASAP**.

3. В правой панели включите переключатель **Интеграция с KASAP**.

4. Укажите параметры, которые будут использоваться для подключения к KASAP:

   - **API-токен** – токен, который вы создали для доступа к KASAP Open API.
   - **Веб-адрес** – URL для API-запросов, которые вы получили при создании API-токена.
   - **Использовать прокси-сервер** – переключатель, позволяющий использовать прокси-сервер при подключении к KASAP.

     По умолчанию переключатель выключен.

5. При необходимости проверьте указанные вами параметры, нажав на кнопку **Проверить соединение**.

   Отображается статус соединения.

6. Нажмите на кнопку **Сохранить**.

Интеграция с Kaspersky Automated Security Awareness Platform настроена.

После сохранения параметров интеграции KASAP вы можете просмотреть список обучающихся групп KASAP, нажав на кнопку **Просмотреть группы**.

При необходимости вы можете обновить список отображаемых групп, нажав на кнопку **Обновить группы**.

Открытый список невозможно скрыть. Если вы выключите переключатель **Интеграция с KASAP**, список групп KASAP не будет отображаться.

Настройка интеграции с Kaspersky Threat Intelligence Portal Sandbox

Интеграция с Kaspersky Threat Intelligence Portal (далее также Kaspersky TIP) позволяет запускать исполняемые файлы, перемещенные в раздел **Карантин**, с помощью Kaspersky Sandbox – безопасной среды, изолированной от вашей корпоративной сети.

Параметры интеграции не наследуются, а применяются только к Серверу администрирования (физическому или виртуальному), на котором вы настраиваете эти параметры.

Перед настройкой интеграции вам нужно получить токен авторизации для API-запросов на Kaspersky TIP.

Чтобы настроить интеграцию с Kaspersky TIP Sandbox:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Выберите **Kaspersky TIP**.

3. В правой панели включите переключатель **Интеграция**.

   Отобразятся параметры подключения к Kaspersky TIP.

   Если после настройки и сохранения параметров интеграции вы выключите переключатель **Интеграция**, параметры не удаляются, но выполнить действие по реагированию будет невозможно.

4. Нажмите кнопку **Добавить токен**, в открывшемся окне укажите токен, ранее полученный на Kaspersky TIP, а затем нажмите кнопку **Добавить**.

   API-токен добавлен.

5. Если вы хотите использовать прокси-сервер при подключении к Kaspersky TIP, включите переключатель **Использовать прокси-сервер**.

   По умолчанию переключатель выключен.

6. Нажмите на кнопку **Сохранить**.

Интеграция с Kaspersky TIP Sandbox будет настроена.

Теперь вы можете отправлять файлы из раздела **Карантин** в Kaspersky TIP Sandbox для анализа угроз. Максимальный размер файла составляет 100 МБ.

Поскольку лицензия Kaspersky Security для бизнеса Профессиональный поддерживает мультитенантность, файлы, помещенные в **Карантин**, делятся по тенантам. Это разделение на уровне тенантов также применяется при отправке файлов в Kaspersky TIP Sandbox и при просмотре результатов, если администратор использует выделенную учетную запись Kaspersky TIP и API-токен, связанный с каждым тенантом. Однако централизованное управление разделом **Карантин** для всех тенантов невозможно, так как в списке объектов помещенных на карантин не отображаются объекты в соответствии с иерархией Сервера.

Группировка алертов по атрибутам

Агрегирование алертов помогает идентифицировать алерты, которые могут быть связаны с одним и тем же инцидентом, что упрощает процесс расследования.

Чтобы включить функцию агрегирования алертов, вам нужно выполнить следующее:

- Включить подраздел **Алерты** в главном меню.
- Активировать Сервер администрирования по лицензии Kaspersky Security для бизнеса Профессиональный, а затем распространить лицензионный ключ Kaspersky Security для бизнеса Профессиональный на управляемые приложения.

  При использовании функциональности по пробной лицензии Kaspersky Security для бизнеса Профессиональный вам нужно сначала добавить физический подчиненный Сервер администрирования, а затем активировать этот Сервер по этой лицензии.

Если у вас есть лицензии Kaspersky Next EDR Optimum, вам не нужно активировать приложения, установленные на ваших управляемых устройствах по лицензии Kaspersky Security для бизнеса Профессиональный. Вам нужно выполнить это только для новых устройств, если они есть. Поскольку лицензия Kaspersky Security для бизнеса Профессиональный поддерживает мультитенантность, вы можете централизованно распространять лицензионный ключ среди управляемых приложений. Автоматическое распространение лицензии на подчиненные и виртуальные Серверы администрирования не поддерживается.

Вы можете агрегировать алерты по имени устройства, учетной записи или SHA256.

> Алерты объединяются по атрибуту, только если этот атрибут не пуст.

Алерты объединяются, если они имеют хотя бы один атрибут и возникают в течение 24 часов после любого другого алерта в группе.

Чтобы агрегировать алерты по атрибутам:

1. В главном окне приложения перейдите в раздел **Мониторинг → Алерты**.
2. Выполните одно из следующих действий:
   - Включите переключатель **Агрегация алертов** и выберите один или несколько атрибутов, по которым нужно агрегировать алерты:
     - **Имя устройства**
     - **Учетная запись**
     - **Хеш файла (SHA256)**

     По умолчанию выбраны атрибуты **Имя устройства** и **Учетная запись**.
   - Нажмите на значок параметров (⚙). В открывшейся панели **Параметры таблицы** перейдите на вкладку **Группировка**. Выберите **Идентификатор группы агрегации** и нажмите **Применить**.

Когда агрегация включена, алерты сортируются по параметру **Время события** от самого нового к самому старому. Дополнительные параметры сортировки не поддерживаются. Выбор другой группы параметров выключит агрегацию.

В таблице отображаются алерты, сгруппированные по атрибутам. Неагрегированные алерты перечислены внизу таблицы.

Каждый алерт назначается только одной группе после агрегирования.

Cloud Discovery

Kaspersky Security Center Linux позволяет отслеживать использование облачных сервисов на управляемых устройствах с операционной системой Windows и блокировать доступ к нежелательным облачным сервисам. Cloud Discovery отслеживает попытки пользователей получить доступ к этим службам через браузеры и настольные приложения. Также отслеживает попытки доступа пользователей к облачным сервисам через незашифрованные соединения (например, по протоколу HTTP). Эта функция позволяет выявлять и прекращать скрытое несанкционированное использование облачных сервисов.

Возможность блокировки доступна только в том случае, если вы активировали Kaspersky Security Center Linux по лицензии Kaspersky Next EDR Optimum или Kaspersky Symphony XDR.

Возможность блокировки доступна только при использовании Kaspersky Endpoint Security 11.2 для Windows и выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.

Можно включить функцию Cloud Discovery и выбрать политики безопасности или профили, для которых ее требуется включить. Можно также включать и выключать функцию отдельно для каждой политики безопасности или профиля. Вы можете заблокировать доступ к облачным сервисам, к которым вы хотите ограничить доступ для пользователей.

Чтобы заблокировать доступ к нежелательным облачным сервисам, убедитесь, что выполнены следующие условия:

- Вы используете версию Kaspersky Endpoint Security 11.2 для Windows или выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.
- Вы приобрели лицензию на Kaspersky, которая дает возможность блокировать доступ к нежелательным облачным сервисам. Подробную информацию см. в справке Kaspersky.

Информация об удачных и заблокированных попытках доступа к облачным сервисам отображается в виджете Cloud Discovery и в отчетах Cloud Discovery. Виджет также показывает уровень риска каждого облачного сервиса. Kaspersky Security Center Linux получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных профилями безопасности, в которых они включены.

Включение функции Cloud Discovery с помощью виджета

Функция Cloud Discovery получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных политиками безопасности, в которых она включена. Включить или выключить Cloud Discovery можно только для политики Kaspersky Endpoint Security для Windows.

Существуют два способа включить функцию Cloud Discovery:

- С помощью виджета Cloud Discovery.
- В свойствах политики Kaspersky Endpoint Security для Windows.

  Подробную информацию о том, как включить функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security для Windows, см. в разделе Cloud Discovery справки Kaspersky Endpoint Security для Windows.

Обратите внимание, что вы можете выключить функцию Cloud Discovery только в параметрах политики Kaspersky Endpoint Security для Windows.

Чтобы включить Cloud Discovery, у вас должно быть право **Запись** в функциональной области **Общие функции: Базовая функциональность**.

Чтобы включить функцию Cloud Discovery с помощью виджета Cloud Discovery:

1. Откройте Kaspersky Security Center Linux.
2. В главном окне приложения перейдите в раздел **Мониторинг → Панель мониторинга**.
3. В виджете **Cloud Discovery** нажмите на кнопку **Включить**.

   Если у вас установлен Kaspersky Endpoint Security для Windows версии 12.4, включите функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security для Windows. Подробнее см. раздел Cloud Discovery справки Kaspersky Endpoint Security для Windows.

   Если у вас версия Kaspersky Endpoint Security для Windows ниже версии 12.4, обновите плагин Kaspersky Endpoint Security для Windows до версии 12.5.

4. В открывшемся окне **Включить Cloud Discovery** выберите политики безопасности, для которых вы хотите включить функцию и нажмите на кнопку **Включить**.

   Следующие параметры политики будут включены автоматически: **Внедрение скрипта в веб-трафик для взаимодействия с веб-страницами**, **Мониторинг веб-сеансов** и **Проверка зашифрованных подключений**.

Функция Cloud Discovery включена, виджет добавлен в панель мониторинга.

Добавление виджета Cloud Discovery в панель мониторинга

Вы можете добавить виджет **Cloud Discovery** в панель мониторинга, чтобы отслеживать использование облачных сервисов на управляемых устройствах.

Чтобы добавить виджет Cloud Discovery в панель мониторинга, у вас должно быть право **Запись** в функциональной области **Общие функции: Базовая функциональность**.

Чтобы добавить виджет Cloud Discovery в панель мониторинга:

1. Откройте Kaspersky Security Center Linux.
2. В главном окне приложения перейдите в раздел **Мониторинг → Панель мониторинга**.
3. Нажмите на кнопку **Добавить или восстановить виджет**.
4. В списке доступных виджетов нажмите на значок шеврона (>) рядом с категорией **Другое**.
5. Выберите виджет **Cloud Discovery** и нажмите на кнопку **Добавить**.

   Если функция Cloud Discovery выключена, следуйте инструкциям в разделе Включение функции Cloud Discovery с помощью виджета.

Выбранный виджет будет добавлен в конец панели мониторинга.

Просмотр информации об использовании облачных сервисов

Виджет **Cloud Discovery** показывает информацию о попытках доступа к облачным сервисам. Виджет также показывает уровень риска каждого облачного сервиса. Kaspersky Security Center Linux получает информацию об использовании облачных сервисов со всех управляемых устройств, защищенных только теми профилями безопасности, в которых включена эта функция.

Перед просмотром убедитесь, что:

- Виджет Cloud Discovery добавлен в панель мониторинга.
- Функция Cloud Discovery включена.
- У вас есть право **Чтение** в функциональной области **Общие функции: Базовая функциональность**.

Чтобы посмотреть виджет Cloud Discovery:

1. Откройте Kaspersky Security Center Linux.
2. В главном окне приложения перейдите в раздел **Мониторинг → Панель мониторинга**.

   Виджет **Cloud Discovery** отображается в панели мониторинга.

3. В левой части виджета **Cloud Discovery** выберите категорию облачных сервисов.

   В таблице в правой части виджета отображается до пяти сервисов из выбранной категории, к которым пользователи чаще всего пытаются получить доступ. Учитываются как успешные, так и заблокированные попытки доступа.

4. В правой части виджета выберите требуемый сервис.

   В таблице ниже отображается до десяти устройств, наиболее часто обращающихся к этому сервису. В этой таблице вы можете сформировать два типа отчетов: отчет об успешных попытках доступа и отчет о заблокированных попытках доступа.

   Также в этой таблице вы можете заблокировать доступ к облачной службе для определенного устройства.

В виджете отображаются запрашиваемые данные.

В отображаемом виджете можно выполнить следующие действия:

- Перейдите в раздел **Мониторинг** → **Отчеты**, чтобы просмотреть отчеты Cloud Discovery.
- Заблокируйте или разрешите доступ к выбранному облачному сервису.

Возможность блокировки доступна только в том случае, если вы активировали Kaspersky Security Center Linux по лицензии Kaspersky Next EDR Optimum или Kaspersky Symphony XDR.
Возможность блокировки доступна только при использовании Kaspersky Endpoint Security 11.2 для Windows и выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.

Уровень риска облачных сервисов

Cloud Discovery определяет уровень риска для каждого облачного сервиса. Уровень риска помогает определить сервисы, не соответствующие требованиям безопасности вашей организации. Например, вы можете принять во внимание уровень риска при принятии решения о блокировке доступа к определенному сервису.

Уровень риска является оценочным показателем и ничего не говорит о качестве облачного сервиса или о производителе. Уровень риска – это рекомендация экспертов "Лаборатории Касперского".

Уровни риска облачных сервисов отображаются в виджете Cloud Discovery и в списке всех контролируемых облачных сервисов.

Блокировка доступа к нежелательным облачным сервисам

Вы можете заблокировать доступ к облачным сервисам, к которым вы хотите ограничить доступ для пользователей. Вы также можете разрешить доступ к облачным сервисам, которые ранее были заблокированы.

Например, уровень риска можно учесть при принятии решения о блокировке доступа к определенному сервису.

Вы можете заблокировать или разрешить доступ к облачным сервисам для политики безопасности или профиля политики.

Существует два способа заблокировать доступ к нежелательным облачным сервисам:

- С помощью виджета Cloud Discovery.

  В этом случае вы можете заблокировать доступ к сервисам по очереди.

- В свойствах политики Kaspersky Endpoint Security для Windows.

  В этом случае вы можете заблокировать доступ к сервисам по очереди или сразу всю категорию.

  Подробную информацию о том, как включить функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security для Windows, см. в разделе Cloud Discovery справки Kaspersky Endpoint Security для Windows.

Чтобы заблокировать или разрешить доступ к облачному сервису с помощью виджета:

1. Откройте виджет Cloud Discovery и выберите требуемый облачный сервис.
2. В панели **Топ 10 устройств, использующих эту службу** найдите политику безопасности или профиль политики, для которых вы хотите заблокировать или разрешить службу.
3. В соответствующей строке в столбце **Статус доступа в политике или профиле политики** выполните одно из следующих действий:
   - Чтобы заблокировать службу, в раскрывающемся списке выберите **Заблокировано**.
   - Чтобы разрешить службу, в раскрывающемся списке выберите **Разрешено**.
4. Нажмите на кнопку **Сохранить**.

Доступ к выбранной службе заблокирован или разрешен для политики безопасности или профиля политики.

Экспорт событий в SIEM-системы

В этом разделе описывается, как настроить экспорт событий в SIEM-системы.

Настройка экспорта событий в SIEM-системы

Kaspersky Security Center Linux позволяет выполнять настройку экспорта событий в SIEM-системы одним из следующих способов: экспорт в любую SIEM-систему, использующую формат syslog, экспорт в Kaspersky SIEM (KUMA), QRadar, Splunk, ArcSight SIEM-системы, использующие форматы LEEF и CEF, или экспорт событий в SIEM-системы прямо 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 приложениях "Лаборатории Касперского". Затем можно отметить события для экспорта для определенного управляемого приложения.

- **Настройка экспорта событий в SIEM-систему**

  Экспортировать события можно следующими способами:

  - Использование протоколов TCP, 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

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 приложений "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования.

Вы можете использовать экспорт событий в централизованных системах, работающих с вопросами безопасности на организационном и техническом уровнях, обеспечивающих мониторинг систем безопасности и консолидирующих данные из различных решений. К ним относятся SIEM-системы, обеспечивающие анализ алертов систем безопасности и событий сетевого аппаратного обеспечения и приложений в режиме реального времени, а также центры управления безопасностью (Security Operation Center, SOC).

SIEM-системы получают данные из многих источников, включая сети, системы безопасности, серверы, базы данных и приложения. Они также обеспечивают функцию объединения обработанных данных, что не позволит вам пропустить критические события. Кроме того, эти системы выполняют автоматический анализ связанных событий и сигналов тревоги для уведомления администраторов о вопросах системы безопасности, требующих незамедлительного решения. Уведомления могут отображаться в панели индикаторов или рассылаться по сторонним каналам, например, по электронной почте.

В процедуре экспорта событий из Kaspersky Security Center 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.

Способы отправки событий из Kaspersky Security Center Linux

Существует три способа отправки событий из Kaspersky Security Center Linux во внешние системы:

- Отправка событий по протоколу Syslog в любую SIEM-систему.

  Используя протокол Syslog, вы можете передавать любые события, произошедшие на Сервере администрирования и в приложениях "Лаборатории Касперского", установленных на управляемых устройствах. Протокол Syslog – это стандартный протокол регистрации сообщений. Вы можете использовать этот протокол для экспорта событий в любую SIEM-систему.

  Для этого нужно отметить события, которые вы хотите передать в SIEM-систему. Вы можете отметить события в Kaspersky Security Center Web Console. Только отмеченные события будут передаваться в SIEM-систему. Если вы ничего не отметили, никакие события не будут передаваться.

- Отправка событий по протоколам CEF и LEEF в системы Kaspersky SIEM, QRadar, Splunk и ArcSight

  Протоколы CEF и LEEF можно использовать для экспорта общих событий. При экспорте событий по протоколам CEF и LEEF у вас нет возможности выбора определенных экспортируемых событий. Вместо этого выполняется экспорт всех общих событий. Для конвертации событий Kaspersky Security Center Linux в события формата CEF и LEEF используется файл siem_conversion_rules.xml. Этот файл содержит список атрибутов событий Kaspersky Security Center Linux и соответствующие атрибуты событий в формате CEF и LEEF. Также файл siem_conversion_rules.xml содержит правила генерации сообщений, соответствующих событиям. Этот файл входит в комплект поставки Kaspersky Security Center Linux.

  В отличие от протокола Syslog, протоколы CEF и LEEF не являются универсальными. Протоколы CEF и LEEF предназначены для соответствующих SIEM-систем (Kaspersky SIEM (KUMA), QRadar, Splunk и ArcSight). Поэтому при выборе экспорта событий по одному из этих протоколов в SIEM-системе используется нужный анализатор.

- Напрямую из базы данных Kaspersky Security Center Linux в любую SIEM-систему.

  Этот способ экспорта событий можно использовать для получения событий напрямую из публичных представлений базы данных с помощью SQL-запросов. Результаты выполнения запроса сохраняются в .xml файл, который можно использовать в качестве входных данных для внешней системы. Напрямую из базы данных можно экспортировать только события, доступные в публичных представлениях.

Получение событий SIEM-системой

SIEM-система должна принимать и корректно анализировать события, получаемые из Kaspersky Security Center Linux. Для этого необходимо правильно настроить SIEM-систему. 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**

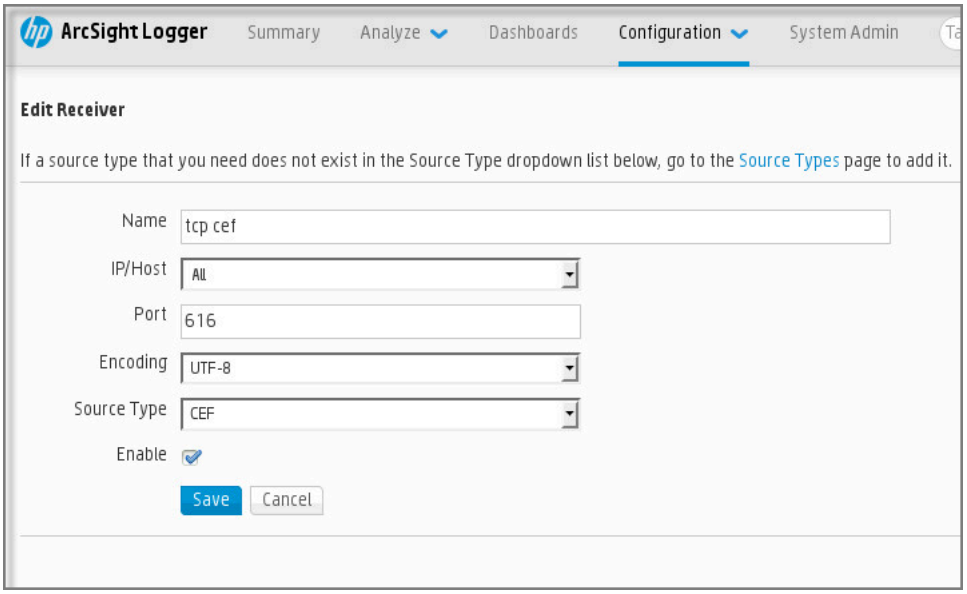
  Укажите номер порта для подключения к Kaspersky Security Center Linux. Этот порт должен совпадать с портом, который вы указываете в Kaspersky Security Center Linux при настройке экспорта событий в SIEM-систему.

- **Формат даты**

  Укажите формат syslog, CEF или LEEF.

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, чтобы информация о событиях могла быть использована SIEM-системой. Анализатор сообщений встроен в SIEM-систему; он используется для разбиения содержимого сообщения на соответствующие поля, такие как код события, 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.

Об экспорте событий в форматах CEF и LEEF

Форматы CEF и LEEF можно использовать для экспорта в SIEM-систему общих событий, событий изменения политик и событий, переданных приложениями "Лаборатории Касперского" Серверу администрирования. Набор экспортируемых событий определен заранее, возможность выбирать экспортируемые события отсутствует. Перед отправкой событий в SIEM-систему (Kaspersky SIEM (KUMA), QRadar, ArcSight или Splunk) необходимо интерпретировать события Kaspersky Security Center Linux в события в формате CEF и LEEF, используя правила, указанные в файле siem_conversion_rules.xml.

Формат экспорта можно выбрать в зависимости от того, какую SIEM-систему вы используете. В следующей таблице приведены SIEM-системы и соответствующие им форматы экспорта.

Форматы экспорта событий в SIEM-систему

SIEM-система	Формат экспорта
Kaspersky SIEM	CEF
ArcSight	CEF
Splunk	CEF
QRadar	LEEF

- LEEF (Log Event Extended Format) – это специализированный формат событий для IBM Security QRadar SIEM. QRadar может получать, идентифицировать и обрабатывать события, передаваемые по протоколу LEEF. Для протокола LEEF должна использоваться кодировка UTF-8. Более подробную информацию о протоколе LEEF см. на веб-странице IBM Knowledge Center.

- CEF – это стандарт управления типа "открытый журнал", который улучшает совместимость информации системы безопасности от разных сетевых устройств и приложений. Протокол CEF позволяет использовать общий формат журнала событий, чтобы системы управления предприятием могли легко получать и объединять данные для анализа. Для протокола CEF должна использоваться кодировка UTF-8.

При автоматическом экспорте Kaspersky Security Center Linux отправляет общие события в SIEM-систему. Автоматический экспорт событий начинается сразу после включения. В этом разделе описана процедура включения автоматического экспорта событий.

Конвертация событий в формат CEF или LEEF

Перед отправкой событий в SIEM-систему (Kaspersky SIEM (KUMA), QRadar, ArcSight или Splunk) необходимо интерпретировать события Kaspersky Security Center Linux в события в формате CEF и LEEF, используя правила, указанные в файле siem_conversion_rules.xml. Этот файл входит в комплект поставки Kaspersky Security Center Linux.

Файл siem_conversion_rules.xml содержит предустановленные правила интерпретации для конвертации событий в формат CEF и LEEF. Если вы хотите использовать дополнительные правила интерпретации событий, вы можете добавить их в файл вручную.

Файл siem_conversion_rules.xml включает следующие секции:

- `<product name="SP_QRADAR" vendor="IBM">`

  Эта секция содержит правила генерации событий в формате LEEF, которые можно экспортировать в SIEM-систему QRadar.

- `<product name="SP_ARCSIGHT" vendor="HP">`.

  Эта секция содержит правила генерации событий в формате CEF, которые можно экспортировать в SIEM-систему ArcSight или Splunk.

- `<product name="Kaspersky SIEM" vendor="Kaspersky">`.

  Эта секция содержит правила генерации событий в формате CEF, которые можно экспортировать в KUMA.

В каждом разделе есть подраздел `<common>`, в котором размещены атрибуты событий Kaspersky Security Center Linux и соответствующие им атрибуты событий в формате LEEF. Эти общие атрибуты используются для всех типов событий, которые можно экспортировать.

Каждый раздел также имеет подраздел `<event>`. Каждый подраздел `<event>` содержит дополнительные атрибуты, которые добавляются к атрибутам, указанным в разделе `<common>`.

Вы можете вручную добавить новое правило генерации событий в файл siem_conversion_rules.xml.

Чтобы добавить новое правило генерации событий:

1. Добавьте новый подсекцию `<event>` в секцию `<product name="SP_QRADAR" vendor="IBM">`, `<product name="SP_QRADAR" vendor="IBM">` или `<product name="Kaspersky SIEM" vendor="Kaspersky">`, а затем укажите дополнительные атрибуты события, если необходимо.

2. Если событие состоит только из общих атрибутов, подраздел `<event>` будет пустым.

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Generation rule for the GNRL_EV_VIRUS_FOUND event with additional
attributes -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
    <product name="Kaspersky SIEM" vendor="Kaspersky">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

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 приложениях, управляемых данной политикой. Если экспортируемые события были выбраны в политике, вам не удастся их переопределить для отдельного приложения, управляемой этой политикой.

- Выбор событий для управляемого приложения. Если вы выбираете экспортируемые события для управляемого приложения, установленного на управляемых устройствах, то в SIEM-систему будут переданы только события, которые произошли в этом приложении.

Для событий изменения политик вы можете только включить или выключить экспорт всех таких событий в SIEM-систему.

Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog

Если вы хотите выполнить экспорт событий, произошедших в определенном управляемом приложении, установленном на управляемых устройствах, выберите события для экспорта политике приложения. В этом случае отмеченные события экспортируются со всех устройств, входящих в область действия политики.

Чтобы отметить события для экспорта для определенного управляемого приложения:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Выберите политику приложения, для которого нужно отметить события.

   Откроется окно свойств политики.
3. Перейдите в раздел **Настройка событий**.
4. Установите флажки рядом с событиями, которые требуется экспортировать в SIEM-систему.
5. Нажмите на кнопку **Отметить для экспорта в SIEM-систему по протоколу syslog**.

   > Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

6. Флажок (✓) появляется в столбце **Syslog** для события или событий, которые вы отметили для экспорта в SIEM-систему.
7. Нажмите на кнопку **Сохранить**.

Отмеченные события из управляемого приложения готовы к экспорту в SIEM-систему.

Вы можете отметить, какие события экспортировать в SIEM-систему для конкретного управляемого устройства. В случае, если ранее экспортируемые события были выбраны в политике приложения, вам не удастся переопределить выбранные события для управляемого устройства.

Чтобы выбрать события для управляемого устройства:

1. В главном окне приложения перейдите в раздел **Управление активами** → **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 **Приложения**.

4. Перейдите по ссылке с названием требуемого приложения в списке приложений.

5. Перейдите в раздел **Настройка событий**.

6. Установите флажки рядом с событиями, которые требуется экспортировать в SIEM-систему.

7. Нажмите на кнопку **Отметить для экспорта в SIEM-систему по протоколу syslog**.

   Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

8. Флажок (✓) появляется в столбце **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. В главном окне приложения выполните одно из следующих действий:

   - Нажмите на имя Сервера администрирования.
   - Перейдите в раздел **Управление активами** → **Политики**, а затем перейдите по ссылке политики.

2. В открывшемся окне перейдите на вкладку **Настройка событий**.

3. Нажмите **Отметить для экспорта в SIEM-систему по протоколу syslog**.

   Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

4. Флажок (✓) появляется в столбце **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 приложениях "Лаборатории Касперского", установленных на управляемых устройствах.

Syslog – это стандартный протокол регистрации сообщений. Этот протокол позволяет разделить программное обеспечение, генерирующее сообщения, систему, в которой хранятся сообщения, и программное обеспечение, выполняющее анализ и отчетность по сообщениям. Каждому сообщению присваивается код устройства, указывающий тип программного обеспечения, с помощью которого было создано сообщение, и уровень важности.

Формат Syslog определяется документами Request for Comments (RFC), опубликованными Internet Engineering Task Force. Стандарт RFC 5424 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

Для экспорта событий в SIEM-систему необходимо настроить процесс экспорта в Kaspersky Security Center Linux.

Перед отправкой событий в SIEM-систему (Kaspersky SIEM (KUMA), QRadar, ArcSight или Splunk) необходимо интерпретировать события Kaspersky Security Center Linux в события в формате CEF и LEEF, используя правила, указанные в файле siem_conversion_rules.xml.

Чтобы настроить экспорт в SIEM-системы из Kaspersky Security Center Web Console:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Экспорт в SIEM-систему**.

3. Перейдите по ссылке **Настроить подключения**.

   Откроется раздел **Параметры экспорта**.

4. 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 файл 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 Linux. Чтобы добавить отпечаток SHA1, введите его в поле **Отпечатки** и нажмите на кнопку **Добавить**.

       С помощью **Добавить проверку подлинности клиента** вы можете сгенерировать сертификат для аутентификации Kaspersky Security Center Linux. Таким образом, вы будете использовать самоподписанный сертификат, выпущенный Kaspersky Security Center Linux. 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 Linux.

  - **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 Linux. В результате Kaspersky Security Center Linux сохраняет сгенерированный самоподписанный сертификат, и вы можете передать публичную часть сертификата или SHA1-отпечаток в SIEM-систему.

- **Формат данных**

  Вы можете выбрать форматы Kaspersky SIEM (KUMA), IBM QRadar SIEM, ArcSight, Splunk или Syslog в зависимости от требований SIEM-системы.

  Если вы выбрали формат данных системного журнала, вы должны указать **Максимальный размер сообщения в байтах**

  Укажите максимальный размер в байтах одного сообщения, передаваемого в SIEM-систему. Каждое событие передается одним сообщением. Если реальная длина сообщения превышает указанное значение, сообщение обрезается и данные могут быть утеряны. По умолчанию размер сообщения составляет 2048 байт. Это поле доступно, только если вы выбрали формат Syslog в поле **Протокол**.

5. Заархивированные события можно экспортировать из базы данных Сервера администрирования и задать начальную дату, с которой вы хотите начать экспорт заархивированных событий:

   a. Перейдите по ссылке **Установите дату начала экспорта**.

   b. В открывшемся разделе, укажите дату начала экспорта в поле **Дата начала экспорта**.

   c. Нажмите на кнопку **ОК**.

6. Включите параметр **Экспортировать события в SIEM**.

7. Чтобы отправлять события изменения политик в SIEM, включите параметр **Экспорт расширенных событий для изменений политики в SIEM**. Для каждого измененного параметра политики будет отправлено отдельное событие в SIEM.

8. Чтобы убедиться, что соединение с SIEM-системой настроено, нажмите на кнопку **Проверить подключение**.

   Соединение с сервером SIEM-системы установлено, и отправлено тестовое событие. Отобразится статус подключения.

9. Нажмите на кнопку **Сохранить**.

Экспорт в SIEM-систему настроен. Если вы настроили получение событий в SIEM-системе, Сервер администрирования экспортирует выбранные события или события изменения политик в SIEM-систему. Если вы установите дату начала экспорта, Сервер администрирования также экспортирует выбранные события, хранящиеся в базе данных Сервера администрирования, с указанной даты.

Мониторинг изменений политики и профилей политик

При изменении параметра политики генерируется событие изменения политики, которое затем можно экспортировать в SIEM-систему для отслеживания изменений политики и создания алертов. Доступ к событиям изменения политик возможен только через SIEM-систему.

События изменения политик не сохраняются в базе данных Сервера администрирования после генерации и не могут быть просмотрены в Kaspersky Security Center Web Console в разделе **Мониторинг → Выборки событий**. Вы также не можете указать параметры уведомлений и параметры хранилища для этих событий на вкладке **Настройка событий**.

При создании политики событие изменения политики генерируется для каждого параметра политики. При изменении политики событие изменения политики создается для каждого измененного параметра политики. При удалении политики генерируется одно событие. Например, создание политики Kaspersky Security Center сгенерирует около 1000 событий, а создание политики Kaspersky Endpoint Security сгенерирует более 7000 событий.

Условия для генерации событий изменения политик

События изменения политик создаются, когда пользователь совершает с политикой или профилем политики любое из следующих действий:

- Создание, изменение или удаление политики.
- Создание, изменение или удаление профиля политики.
- Откат политики к выбранной ревизии.
- Импорт или копирование политики.
- Импорт или копирование профиля политики.
- Перемещение политики в другую группу администрирования.

События изменения политик генерируются при выполнении следующих условий:

- Изменены политики следующих приложений:
  - Агент администрирования Kaspersky Security Center.
  - Сервер администрирования Kaspersky Security Center.
  - Kaspersky Endpoint Security для Windows 14.1 или более поздней версии.
  - Kaspersky Endpoint Security для Linux 12.5 или более поздней версии.
  - Kaspersky Endpoint Security для Linux 12.4 или более поздней версии.
  - Kaspersky Endpoint Security для Mac 12.2.1 или более поздней версии.
- В свойствах Сервера администрирования включен параметр **Экспорт расширенных событий для изменений политики в SIEM**.
- Изменение политики осуществляется вручную через Kaspersky Security Center Web Console.

События изменения политик не создаются в следующих случаях:

- Изменены общие параметры политики.
- Изменены параметры политики, унаследованные от родительской политики.
- Параметры политики изменены через Kaspersky Security Center OpenAPI.
- Параметры приложения "Лаборатории Касперского" изменены в самом приложении.

Поля событий изменения политики

В таблице ниже показан набор полей события изменения политики. Представление этих полей зависит от формата событий (например, syslog, CEF или LEEF). Точные имена полей и шаблоны событий см. в файле siem_conversion_rules.xml. Параметры события доступны только на английском языке.

Поле события	Тип данных	Описание
`eventType`	string	Тип события. Позволяет создавать правила корреляции для определенного типа событий. Возможные значения: "Policy created", "Policy modified", "Policy deleted".
`srvName`	string	Имя Сервера администрирования.
`eventTime`	datetime	Дата и время события (в формате UTC).
`eventGroupID`	int	Идентификатор изменения группы событий.
`objectID`	int	Внутренний идентификатор объекта.
`objectName`	string	Отображаемое имя политики.
`objectGroup`	string	Полный путь и имя группы администрирования, в которой находится политика.
`user`	string	Имя пользователя, который внес изменения в политику.

`operation`	string	Тип изменения параметра. Возможные значения: "Added", "Removed", "Changed".
`path`	string	Путь к параметру. Содержит путь к родительскому узлу параметра, который был изменен. Путь создается на основе названий разделов и подразделов политики. Структура пути идентична описанной в разделах Параметры политики Агента администрирования, Общие параметры политики и Сравнение ревизий политики.
`parameter`	string	Название параметра политики, который был изменен.
`oldValue`	string	Старое значение параметра политики, который был изменен.
`newValue`	string	Новое значение параметра политики, который был изменен.

Экспорт событий напрямую из базы данных

Вы можете извлекать события напрямую из базы данных Kaspersky Security Center Linux, 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, приложениям, 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 приложения для работы с базами данных для создания SQL-запросов и представлений баз данных. Информация о том, как посмотреть параметры подключения к базе данных Kaspersky Security Center 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. Используйте версию утилиты klsql2, которая входит в вашу установленную версию Kaspersky Security Center Linux.

Чтобы использовать утилиту klsql2:

1. Перейдите в директорию, в которой установлен Сервер администрирования. По умолчанию задан путь /opt/kaspersky/ksc64/sbin.

2. В этой директории создайте пустой файл с расширением .sql.

3. Откройте созданный файл .sql с помощью любого текстового редактора.

4. В файле .sql введите требуемый SQL-запрос и сохраните файл.

5. На устройстве, на котором установлен Сервер администрирования, в командной строке введите следующую команду для выполнения SQL-запроса из файла .sql и сохранения результатов в файл result.xml:

   ```
   sudo ./klsql2 -i src.sql -u <имя пользователя> -p <пароль> -o result.xml
   ```

   где <имя пользователя> и <пароль> являются учетными данными учетной записи пользователя, имеющего доступ к базе данных.

6. При необходимости введите имя учетной записи и пароль пользователя, имеющего доступ к базе данных.

7. Откройте созданные файлы result.xml и просмотрите результаты выполнения SQL-запроса.

Вы можете изменять файл .sql и создавать в нем любые SQL-запросы к публичным представлениям. Затем с помощью команды в командной строке можно запустить 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.

Следующие примеры показывают, как получить список событий, зарегистрированных на устройствах пользователей за последние 7 дней, и отсортировать их по времени возникновения. Сначала отображаются самые последние события.

Пример для PostgreSQL:

```
SELECT
  /* event ID */
  "e"."nId",

  /* time of the event */
  "e"."tmRiseTime",

  /* internal name of the event type */
  "e"."strEventType",

  /* event display name */
  "e"."wstrEventTypeDisplayName",

  /* event display description */
  "e"."wstrDescription",

  /* event display description */
  "e"."wstrGroupName",

  /* display name of the device on which the event occurred */
  "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 address of the device on which the event occurred */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

Пример для MySQL или MariaDB:

```
SELECT

  /* event ID */
  `e`.`nId`,

  /* time of the event */
  `e`.`tmRiseTime`,

  /* internal name of the event type */
  `e`.`strEventType`,

  /* event display name */
  `e`.`wstrEventTypeDisplayName`,

  /* event display description */
  `e`.`wstrDescription`,

  /* device group name */
  `e`.`wstrGroupName`,

  /* display name of the device on which the event occurred */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* IP address of the device on which the event occurred */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
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 окне приложения нажмите на имя 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.

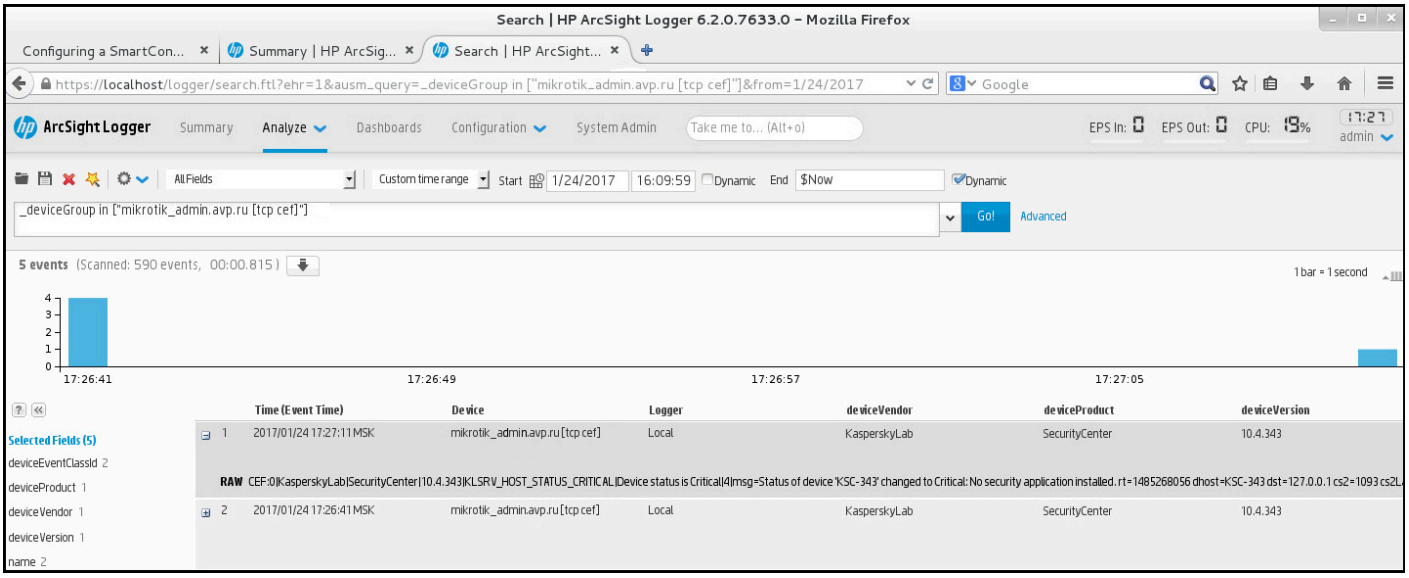
Просмотр результатов экспорта

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

Работа с ревизиями объектов

Этот раздел содержит информацию о работе с ревизиями объектов.

Ревизия – это состояние объекта в определенный момент. Каждый раз, когда вы создаете или изменяете объект, создается новая ревизия этого объекта. Каждая ревизия содержит значения всех параметров объекта, актуальных на момент создания или сохранения ревизии.

Объекты, которые поддерживают работу с ревизиями:

- свойства Сервера администрирования;
- политики;
- задачи;
- группы администрирования;
- учетные записи пользователей;
- инсталляционные пакеты.

Вы можете выполнять с ревизиями объектов следующие действия:

- просматривать выбранную ревизию (доступно только для политик);
- откатывать изменения объекта к выбранной ревизии;
- сохранять ревизии в виде файла JSON (доступно только для политик).

В окне свойств объектов, которые поддерживают работу с ревизиями, в разделе **История ревизий** отображается список ревизий объекта со следующей информацией:

- **Ревизия** – номер ревизии объекта.
- **Время** – дата и время изменения объекта.
- **Пользователь** – имя пользователя, изменившего объект.
- **IP-адрес устройства пользователя** – IP-адрес устройства, с которого был изменен объект.
- **IP-адрес Web Console** – IP-адрес приложения Kaspersky Security Center Web Console, с помощью которого был изменен объект.
- **Действие** – выполненное действие с объектом.
- **Описание** – описание ревизии изменения параметров объекта.

  По умолчанию описание ревизии объекта не заполнено. Чтобы добавить описание ревизии, выберите нужную ревизию и нажмите на кнопку **Изменить описание**. В открывшемся окне введите текст описания ревизии.

Просмотр и сохранение ревизии политики

Ревизия политики — это сохраненное состояние политики, которое автоматически фиксируется каждый раз при ее изменении и сохранении. Ревизия сдержит параметры политики, профили и правила их активации, метаданные о дате, а также пользователе и IP-адресе, которые создали эту ревизию. Kaspersky Security Center Linux позволяет просматривать ревизию политики, чтобы отслеживать изменения настроек, а также сохранять ревизию в файл JSON.

Просмотр и сохранение ревизии политики доступны, если соответствующий веб-плагин управления поддерживает эту функцию.
Опции доступны для политик Сервера администрирования, Агента администрирования, Kaspersky Endpoint Security для Windows (начиная с версии веб-плагина 14.0), Kaspersky Endpoint Security для Linux (начиная с версии веб-плагина 12.4) и Kaspersky Endpoint Security для Mac (начиная с версии веб-плагина 12.2.1 Patch A).

Чтобы просмотреть ревизию политики:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на ревизию политики, которую вы хотите просмотреть и перейдите в раздел **История ревизий**.
3. В списке ревизий политики нажмите на номер ревизии, которую вы хотите просмотреть.

   В открывшемся отчете доступна информация о параметрах политики, ее профилях и правилах активации для них.

   Если размер ревизии превышает 10 МБ, просмотреть ее с помощью Kaspersky Security Center Web Console невозможно. Вам будет предложено сохранить выбранную ревизию в файл JSON.

   Если размер ревизии не превышает 10 МБ, отображается отчет в формате HTML с параметрами выбранной ревизии политики. Так как отчет отображается во всплывающем окне, убедитесь, что в вашем браузере разрешены всплывающие окна.

В случае политик Kaspersky Endpoint Security для Windows и Kaspersky Endpoint Security для Mac в отчете не будет информации о профилях политик.

Чтобы сохранить ревизию политики в файл JSON,

В списке ревизий политики выберите ревизию, которую вы хотите сохранить и нажмите на кнопку **Сохранить в файл**.

Ревизия сохранена в файле JSON.

При необходимости вы можете сравнить ревизии политики.

Сравнение ревизий политики

Вы можете сравнить предыдущие ревизии политики с ее текущей ревизией, сравнить различные ревизии, выбранные в списке, или сравнить ревизию одной политики с ревизией другой политики. Параметры доступны для политик Сервера администрирования, Агента администрирования, Kaspersky Endpoint Security для Windows (начиная с версии веб-плагина 14.0) и Kaspersky Endpoint Security для Mac (начиная с версии веб-плагина 12.2.1 Patch A).

Сравнение ревизий политик доступно, если соответствующие веб-плагины управления поддерживает эту функцию.

Чтобы сравнить ревизии политики:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на политику, ревизии которой вы хотите сравнить.

   Откроется окно свойств политики.
3. Перейдите на вкладку **История ревизий** и установите флажки рядом с ревизиями, которые нужно сравнить.
4. В панели инструментов нажмите на кнопку **Сравнить** и в раскрывающемся списке выберите один из следующих вариантов:

   - **С текущей ревизией**, если вы хотите сравнить ревизию, выбранную на шаге 3, с последней сохраненной ревизией той же политики.
   - **Выбранные ревизии**, если вы хотите сравнить две ревизии, около которых вы установили флажки на шаге 3.

     Порядок установки флажков не влияет на результаты сравнения. По умолчанию более ранняя выбранная ревизия сравнивается с последней ревизией. Например, если вы установите флажки рядом с ревизиями 5 и 1, ревизия 1 будет сравниваться с ревизией 5. Отчет будет содержать информацию о параметрах ревизии 1, которые были добавлены, удалены или изменены по сравнению с ревизией 5.
   - **С ревизией другой политики**, если вы хотите сравнить ревизии двух разных политик.

В открывшейся правой панели выполните следующее:

a. В поле **Название приложения** выберите политику, ревизии которой вы хотите сравнить: Агент администрирования или Сервер администрирования.

b. В поле **Название политики** укажите название политики, ревизию которой вы хотите сравнить с той, которую вы выбрали на шаге 3.

Отобразится список ревизий политики.

c. Выберите нужную ревизию и нажмите на кнопку **Сравнить**.

Отчет сравнения ревизий отобразится в формате HTML на новой вкладке вашего браузера.

Если результат сравнения превышает 10 МБ, отобразится соответствующее диалоговое окно. Вы можете нажать на кнопку **Сохранить в файл**, чтобы сохранить отчет в виде файла, или отменить операцию.

Отчет отображается на языке интерфейса вашего приложения Kaspersky Security Center Web Console. Вы можете развернуть некоторые разделы отчета, нажав на значок стрелки вниз (▾) рядом с разделом или свернуть раздел, нажав на значок стрелки вверх (▴).

Отчет содержит следующую информацию:

- Логотип "Лаборатория Касперского".
- Название отчета.
- Время и дата создания отчета.
- Имя политики, Сервер администрирования и группа администрирования, в которую входит политика (политики), ревизии которой сравнивались.
- Кнопка **Сохранить как HTML**. Если вы нажмете на кнопку, отчет будет сохранен на вашем устройстве.
- Раздел **Сводная информация**, в котором отображается общая информация о сравниваемых ревизиях: имя политики (политик), номер ревизии, время и дата, когда ревизия была сохранена, пользователь, который сохранил ревизию, и описание ревизии.

  Для унаследованных политик пользователь не отображается.

- Различия сравниваемых ревизий. Различия отображаются в следующих разделах:
  - **Добавленные параметры.**
  - **Удаленные параметры.**
  - **Измененные параметры.**
  - **Параметры доступны только для объекта 1** (если вы сравнивали ревизии двух разных политик).
  - **Параметры доступны только для объекта 2** (если вы сравнивали ревизии двух разных политик).

Раздел не отображается, если в нем нет данных.

Откат изменений объекта к предыдущей ревизии

В случае необходимости вы можете откатить изменения объекта. Например, вам может понадобиться вернуть параметры политики к состоянию на определенную дату.

Чтобы откатить изменения объекта:

1. В окне свойств объекта перейдите на вкладку **История ревизий**.
2. В списке ревизий объекта выберите ревизию, к которой нужно откатить изменения.
3. Нажмите на кнопку **Откатить**.
4. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.

   Произойдет откат к выбранной ревизии. В списке ревизий объекта отобразится запись о выполненном действии. В описании ревизии отобразится информация о номере ревизии, к которой вы вернули объект.

Операция отката доступна только для политик и задач.

Активные угрозы

Информация о необработанных файлах, обнаруженных на клиентских устройствах, содержится в разделе **Хранилища**, во вложенном разделе **Активные угрозы**.

Отложенная обработка и дезинфекция выполняются приложением безопасности по запросу или после определенного события. Вы можете настраивать параметры отложенного лечения файлов.

Дезинфекция необработанного файла

Чтобы запустить лечение необработанного файла:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Активные угрозы**.
2. Выполните одно из следующих действий:
   - Установите флажок напротив файла, который вы хотите лечить.
   - Выберите название файла, который нужно лечить.
3. Начните лечение файла, нажав на кнопку **Лечить**.

В результате выполняется попытка лечения выбранного файла.

Если файл вылечен, приложение безопасности, установленное на клиентском устройстве, восстанавливает его в исходную папку. Запись о файле удаляется из списка папки **Активные угрозы**. Если лечение файла невозможно, приложение безопасности, установленное на устройстве, удаляет файл с устройства. Запись о файле удаляется из списка папки **Активные угрозы**.

Возможности лечения и удаления файлов могут различаться в зависимости от установленного приложения безопасности, его версии и параметров.

Скачивание необработанного файла

Kaspersky Security Center Linux позволяет скачать копии необработанных файлов, обнаруженные на клиентских устройствах. Это относится к файлам, которые обрабатываются или удаляются приложением. Файлы скачиваются на устройство с установленным Kaspersky Security Center Linux в указанную папку.

Вы можете скачать копии файлов, если файлы были удалены или изменены во время лечения, а их копии хранятся в хранилище Kaspersky Endpoint Security для Linux на управляемом устройстве.

Чтобы скачать копию необработанного файла:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Активные угрозы**.
2. Выполните одно из следующих действий:
   - Установите флажок напротив файла, который вы хотите скачать.
   - Выберите название файла, который нужно скачать.
3. Начните загрузку, нажав на кнопку **Скачать**.

В результате приложение безопасности клиентского устройства, на котором обнаружен выбранный необработанный файл, скачает копию этого файла в указанную папку.

Удаление файлов из раздела Активные угрозы

*Чтобы удалить файл из раздела **Активные угрозы**:*

1. В главном окне приложения перейдите в раздел **Хранилища** → **Активные угрозы**.
2. Выполните одно из следующих действий:
   - Установите флажок напротив файла, который вы хотите удалить.
   - Выберите название файла, который нужно удалить.
3. Удалите файлы, нажав на кнопку **Удалить**.
4. В открывшемся окне нажмите на кнопку **Удалить**.

   В результате приложения безопасности, поместившие выбранные файлы в хранилища на клиентских устройствах, удаляют файлы из этих хранилищ. Записи о файлах удаляются из списка в папке **Активные угрозы**.

Удаление объектов

В этом разделе приведена информация об удалении объектов.

Вы можете удалять следующие объекты:

- политики;
- задачи;
- инсталляционные пакеты;
- виртуальные Серверы администрирования;
- пользователей;
- группы безопасности;
- группы администрирования.

Чтобы удалить объект:

1. Откройте нужный раздел в Kaspersky Security Center Web Console и выберите объект.
2. В панели инструментов нажмите на кнопку **Удалить**.
3. В появившемся окне нажмите на кнопку **OK**, чтобы подтвердить свой выбор.

   Выбранный объект будет удален.

Когда вы удаляете объект, информация об этом записывается в базу данных. Срок хранения информации об удаленных объектах 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 приложение перемещает устройство в группу Нераспределенные устройства. После удаления устройства установленные приложения "Лаборатории Касперского" – Агент администрирования и приложение безопасности, например Kaspersky Endpoint Security, – остаются на устройстве.

Kaspersky Security Center 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.

  Правила хранения устройств не влияют на устройства, на которых один или несколько дисков зашифрованы с помощью полнодискового шифрования. Такие устройства не удаляются автоматически – вы можете удалить их только вручную. Если вам нужно удалить устройство с зашифрованным жестким диском, сначала расшифруйте диск, а затем удалите устройство.

  > При удалении устройства с зашифрованным жестким диском данные, необходимые для расшифровки диска, также удаляются. Если вы установите флажок **Я понимаю риск и хочу удалить выбранные устройства** в окне подтверждения, которое открывается при удалении таких устройств (из группы **Нераспределенные устройства** или из группы **Управляемые устройства**), это означает, что вы знаете о последующем удалении данных.

  В этом случае для расшифровки диска требуется выполнение следующих условий:

  - Устройство повторно подключается к Серверу администрирования для восстановления данных, необходимых для расшифровки диска.

  - Пользователь устройства помнит пароль для расшифровки.

  - Приложение безопасности, которое использовалось для шифрования диска, например Kaspersky Endpoint Security для Windows, установлено на устройстве.

  Если диск был зашифрован с помощью технологии Kaspersky Disk Encryption, вы также можете попробовать восстановить данные с помощью утилиты FDERT Restore.

> В VDI, если у вас есть устройство с зашифрованными жесткими дисками, информация на зашифрованном диске удаляется после удаления устройства.

При удалении устройства из группы Нераспределенные устройства вручную приложение удаляет устройство из списка. После удаления устройства установленные приложения "Лаборатории Касперского" (если они есть) остаются на устройстве. Затем, если устройство по-прежнему видно Серверу администрирования и вы настроили регулярный опрос сети, Kaspersky Security Center 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.

Загрузка и удаление файлов из разделов Карантин и Файлы резервных копий

В этом разделе представлена информация о том, как загрузить и удалить файлы из разделов Карантин и Файлы резервных копий в Kaspersky Security Center Web Console.

Загрузка файлов из разделов Карантин и Файлы резервного хранилища

Вы можете загрузить файлы из разделов Карантин и Файлы резервного хранилища, только если выполняется одно из двух условий: либо включен параметр **Не разрывать соединение с Сервером администрирования** в свойствах устройства, либо используется шлюз соединения. Иначе загрузка невозможна.

Чтобы сохранить копию файла из раздела Карантин или Файлы резервных копий на жесткий диск:

1. Выполните одно из следующих действий:

   - Если вы хотите сохранить копию файла из Карантина, в главном меню перейдите в раздел **Операции → Хранилища → Карантин**.

   - Если вы хотите сохранить копию файла из Резервного хранилища, в главном меню перейдите в раздел **Операции → Хранилища → Файлы резервных копий**.

2. В открывшемся окне выберите файл, который вы хотите загрузить, и нажмите **Скачать**.

   Начнется загрузка. Копия файла, помещенного в Карантин на клиентском устройстве, сохраняется в указанную папку.

Об удалении объектов из разделов Карантин, Файлы резервного хранилища или Активные угрозы

Когда приложения безопасности "Лаборатории Касперского", установленные на клиентских устройствах, помещают объекты на Карантин, в Резервное хранилище или Активные угрозы, они передают информацию о добавленных объектах в разделы **Карантин**, **Файлы резервных копий** или **Активные угрозы** в Kaspersky Security Center Linux. При открытии одного из этих разделов, вы можете удалить нужный объект.

В разделе **Файлы резервных копий** или **Активные угрозы** выберите объект из списка и нажмите на кнопку **Удалить**.

В разделе **Карантин** можно выполнить одно из следующих действий:

- Установить флажок рядом с именем объекта, который нужно удалить, а затем в панели инструментов нажать на кнопку **Удалить**.
- Нажать на имя объекта, который нужно удалить, и в открывшемся окне свойств в панели инструментов нажать на кнопку **Удалить**.

  В этом случае объект будет удален, на экране отобразится соответствующее уведомление, окно со свойствами закроется.

Kaspersky Security Center Linux либо удаляет выбранный объект из списка, либо удаляет выбранный объект из хранилища. Действие, которое необходимо выполнить, определяется приложением "Лаборатории Касперского", поместившим выбранный объект в хранилище. Приложение "Лаборатории Касперского" указано в поле **Запись добавлена**.

Подробнее о том, какое действие нужно выполнить, см. справку приложения "Лаборатории Касперского".

Управление приложением с помощью SNMP

В этом разделе описывается, как получить информацию от Сервера администрирования с помощью SNMP (Simple Network Management Protocol) в Linux.

SNMP – это протокол управления сетевыми устройствами.

Для работы по SNMP Kaspersky Security Center Linux использует входящую в состав операционной системы службу snmpd и агент SNMP для мониторинга производительности Сервера администрирования и отправки данных сторонним приложениям с помощью OID. Kaspersky Security Center Linux может отправлять эту информацию в виде статистики или SNMP-ловушек, которые представляют собой уведомления о событиях приложения.

SNMP позволяет вам получить доступ к следующей информации о приложении:

- к общей информации;
- статистика Kaspersky Security Center Linux с момента установки приложения;
- информация о событиях Kaspersky Security Center Linux.

> Доступ предоставляется только для чтения.

Информация об SNMP-ловушках и статистика, отправляемая по SNMP, хранятся в файле adminkit.mib. По умолчанию файл adminkit.mib расположен в директории /opt/kaspersky/ksc64/share/snmp/.

Локальная служба snmpd на каждом узле кластера служит SNMP-сервером, который получает статистику. Взаимодействие с внешним SNMP-сервером не поддерживается. SNMP-ловушки могут быть получены с помощью службы snmptrapd локально на каждом узле кластера или перенаправлены на внешний сервер.

Для работы по SNMP предварительно настройте службу snmpd в операционной системе на каждом узле кластера.

Настройка службы snmpd в операционной системе

Перед настройкой убедитесь, что служба snmpd установлена в вашей операционной системе.

Создание учетной записи пользователя для доступа к данным

Перед созданием учетной записи остановите службу snmpd, выполнив следующую команду:

```
bash
sudo systemctl stop snmpd
```

Чтобы обеспечить безопасность доступа к данным по SNMPv3 с аутентификацией и шифрованием, вам нужно создать учетную запись пользователя на стороне службы snmpd со следующей информацией:

- Имя пользователя (с учетом регистра).
- Алгоритм аутентификации (MD5 или SHA, рекомендуется SHA).
- Пароль аутентификации.
- Алгоритм шифрования (поддерживается только AES).
- Пароль шифрования.

Вы можете создать учетную запись пользователя следующими способами:

- С помощью утилиты net-snmp-create-v3-user, если она доступна в операционной системе.
- Вручную, добавив соответствующую директиву в конфигурационный файл службы snmpd.

Чтобы создать учетную запись пользователя с помощью утилиты net-snmp-create-v3-user, выполните следующую команду:

```
net-snmp-create-v3-user -ro -a <алгоритм аутентификации> -x <алгоритм шифрования> <имя пользователя>
```

Пароли аутентификации и шифрования запрашиваются в интерактивно.

Например:

```
net-snmp-create-v3-user -ro -a SHA -x AES MonitoringUser
```

Чтобы создать учетную запись пользователя вручную:

1. Создайте конфигурационный файл /var/lib/snmp/snmpd.conf, выполнив следующую команду:

   ```
   touch /var/lib/snmp/snmpd.conf
   ```

2. Добавьте в конфигурационный файл следующие строки:

   ```
   createUser <имя пользователя> <алгоритм аутентификации> "<пароль аутентификации>" <алгоритм шифрования> "
   <пароль шифрования>"
   ```

   Например:

   ```
   createUser MonitoringUser SHA "MonitoringAuthSecret" AES "MonitoringPrivSecret"
   ```

Создание учетной записи пользователя для получения SNMP-ловушек

Чтобы получать SNMP-ловушки по протоколу SNMPv3 с аутентификацией и шифрованием, вам нужно создать учетную запись на стороне системы мониторинга в контексте соответствующей службы (обычно это служба snmptrapd).

Учетная запись должна содержать следующую информацию:

- Имя пользователя.
- Алгоритм аутентификации.
- Пароль аутентификации.
- Алгоритм шифрования.
- Пароль шифрования.

> В целях безопасности используйте отдельные учетные записи пользователей для доступа к данным и для получения SNMP-ловушек.

Инструкции по созданию учетной записи пользователя для получения SNMP-ловушек см. в документации вашей системы мониторинга.

Настройка службы snmpd

Конфигурация службы snmpd хранится в файле /etc/snmp/snmpd.conf. Вы можете добавить необходимую информацию в существующий конфигурационный файл или создать конфигурационный файл и добавить строки, перечисленные ниже, в указанном порядке.

Если вы решили создать конфигурационный файл, убедитесь, что только суперпользователь имеет к нему доступ. Если нужные права доступа не установлены, настройте их, выполнив следующие команды в указанном порядке:

```
chown root:root /etc/snmp/snmpd.conf
chmod 600 /etc/snmp/snmpd.conf
```

Чтобы настроить службу snmpd:

1. В конфигурационном файле укажите протокол, адрес сетевого интерфейса и номер порта, на котором служба snmpd должна прослушивать входящие запросы.

   - Если вы хотите прослушивать запросы на всех интерфейсах сети, добавьте в конфигурационный файл следующие строки:

     ```
     agentAddress udp:161
     ```

   - Если вы хотите прослушивать запросы только на локальном сетевом интерфейсе, например, если система мониторинга установлена на том же устройстве, добавьте следующие строки в конфигурационный файл:

     ```
     agentAddress udp:127.0.0.1:161
     ```

2. Настройте взаимодействие Kaspersky Security Center Linux со службой snmpd. Вы можете использовать сокет UNIX или сокет TCP.

   - Если вы используете сокет UNIX:

     a. Укажите путь и разрешения для сокета UNIX. Для этого добавьте в конфигурационный файл следующие строки:

     ```
     master agentx
     agentXSocket unix:/var/run/agentx-master.socket
     agentXPerms 770 770 kluser klusers
     ```

     b. Добавьте группу klusers в качестве дополнительной группы для учетной записи {'KLSRV_UNATT_KLSVCUSER'}.

   - Если вы используете сокет TCP, укажите порт и адрес для этого сокета TCP. Для этого добавьте в конфигурационный файл следующие строки:

     ```
     master agentx
     agentXSocket tcp:127.0.0.1:705,tcp6:[::1]:705
     ```

3. Установите минимальное время ожидания ответа не менее 30 секунд. Для этого добавьте в конфигурационный файл следующие строки:

```
agentxTimeout 30
```

4. При необходимости вы можете предоставить описание сервера, на котором настроен SNMP, местоположение системы и контакт администратора. Для этого добавьте в конфигурационный файл следующие строки:

```
sysDescr <описание сервера>
sysLocation <расположение сервера>
sysContact <контакт администратора>
sysServices 72
```

5. Укажите область OID-дерева, которую вы хотите сделать доступной для вашей системы мониторинга по протоколу SNMP. Для этого добавьте в конфигурационный файл следующие строки:

```
view monitoring included .1.3.6.1.4.1.23668.1093.1

view systemonly included .1.3.6.1.4.1.23668.1093.1
```

6. При необходимости вы можете дополнительно указать область OID-дерева, содержащего информацию об операционной системе, которая хранится службой snmpd. Эта область будет доступна вашей системе мониторинга.

   Информация об операционной системе включает, например, информацию об использовании процессора и оперативной памяти, свободном месте на разделах диска, загрузке сетевых интерфейсов, список установленного программного обеспечения, список открытых сетевых подключений и список запущенных процессов. Часть этой информации может быть конфиденциальной.

   - Если вы хотите разрешить доступ только к общей системной информации и информации об использовании оперативной памяти, процессора и дисковых устройств, добавьте следующие строки в конфигурационный файл:

     ```
     # SNMPv2-MIB - Basic system information
     view monitoring included .1.3.6.1.2.1.1
     # HOST-RESOURCES-MIB - CPU, Memory, Filesystems
     view monitoring included .1.3.6.1.2.1.25.1
     view monitoring included .1.3.6.1.2.1.25.2
     view monitoring included .1.3.6.1.2.1.25.3
     view monitoring included .1.3.6.1.2.1.25.5
     # UCD-SNMP-MIB - Memory and CPU usage
     view monitoring included .1.3.6.1.4.1.2021.4
     view monitoring included .1.3.6.1.4.1.2021.10
     view monitoring included .1.3.6.1.4.1.2021.11
     # UCD-SNMP-DISKIO-MIB - Block devices I/O statistics
     view monitoring included .1.3.6.1.4.1.2021.13
     # IF-MIB - Network interfaces I/O statistics
     view monitoring included .1.3.6.1.2.1.2
     view monitoring included .1.3.6.1.2.1.31
     ```

   - Если вы хотите разрешить доступ ко всей системной информации, добавьте следующие строки в конфигурационный файл:

     ```
     view monitoring included .1
     ```

7. Укажите режим доступа и объем информации для созданной учетной записи пользователя. Для этого добавьте в конфигурационный файл следующие строки:

```
rouser <user name> priv -V monitoring
```

8. Чтобы отправить SNMP-ловушки, укажите IP-адрес системы мониторинга и учетные данные пользователя для получения ловушек. Для этого добавьте в конфигурационный файл следующие строки:

```
trapsess -Ci -v3 -t0.1 -r1 -l authPriv -u <имя пользователя для получения ловушек> -a <алгоритм аутентификации>
-A "<пароль пользователя для получения ловушек>" -x <алгоритм шифрования> -X "<пароль шифрования>" udp:<IP
address>:162
```

Служба snmpd настроена.

Для интеграции с несколькими системами мониторинга создайте отдельную учетную запись пользователя для каждой системы, укажите объем доступной информации для каждой учетной записи пользователя (директивы view и rouser) и настройте отправку SNMP-ловушек (директива trapsess).

Запуск службы snmpd с новой конфигурацией

Чтобы применить новую конфигурацию:

1. Перезапустите службу snmpd:

```
systemctl restart snmpd
```

2. Проверьте статус службы snmpd:

```
systemctl status snmpd
```

Статус должен быть `running`.

3. Разрешить автоматический запуск службы при запуске операционной системы:

```
systemctl enable snmpd
```

4. Если вы используете сетевой экран в своей операционной системе или сетевом оборудовании, добавьте правила, позволяющие пропускать пакеты SNMP.

Служба snmpd запущена.

Если служба klcssnmp работала во время настройки службы snmpd, перезагрузите также службу klcssnmp.

Проверка работоспособности службы snmpd

Чтобы протестировать службу snmpd, настройте использование SNMP в Kaspersky Security Center Linux и запросите данные SNMP с помощью утилиты snmpwalk.

Чтобы получить данные SNMP, предоставляемые Kaspersky Security Center Linux,

выполните следующую команду:

```
snmpwalk -v3 -l authPriv -u <имя пользователя> -a <алгоритм аутентификации> -A "<пароль аутентификации>" -x
<алгоритм шифрования> -X "<пароль шифрования>" <IP-адрес> .1.3.6.1.4.1.23668.1093.1
```

Например:

```
snmpwalk -v3 -l authPriv -u MonitoringUser -a SHA -A "MonitoringAuthSecret" -x AES -X "MonitoringPrivSecret"
127.0.0.1 .1.3.6.1.4.1.23668.1093.1
```

Включение и выключение уведомления по SNMP

Kaspersky Security Center Linux отправляет уведомления о событиях Сервера администрирования в виде SNMP-ловушек.

По умолчанию уведомления SNMP о событиях Kaspersky Security Center Linux выключены.

Чтобы включить или выключить уведомление по SNMP о событиях Kaspersky Security Center Linux:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно **Свойства Сервера администрирования**.

2. В окне свойств на вкладке **Настройка событий** выберите тип события, для которого вы хотите получать уведомления SNMP.

3. В открывшейся панели включите или выключите переключатель **Уведомлять по SNMP**.

   Этот параметр доступен, только если включен параметр **Отправка статистики по протоколу SNMP**.

Уведомления SNMP о событиях Kaspersky Security Center Linux будут включены или выключены в соответствии с вашим выбором.

Включение и выключение SNMP в Kaspersky Security Center Linux

По умолчанию отправка статистики по SNMP включена. Чтобы отправлять SNMP-ловушки, настройте службу snmpd.

Чтобы включить или выключить отправку статистики по SNMP:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно **Свойства Сервера администрирования**.

2. На вкладке **Общие** выберите раздел **SNMP**.

3. Включите или выключите переключатель **Отправка статистики по протоколу SNMP**.

4. Нажмите на кнопку **Сохранить**.

Отправка статистики по SNMP будет включена или выключена в зависимости от вашего выбора.

Значения идентификаторов объектов для SNMP

В таблице ниже приведены значения и описания идентификатора объекта (далее также OID), которые используются для передачи информации о производительности Сервера администрирования приложениям сторонних производителей.

Значения и описания параметров идентификаторов объектов для SNMP

Значение идентификатора объекта	Числовой тип данных	OID	Описание
`deploymentStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.1.1	Статус развертывания. Статус может принимать одно из следующих значений: • **Информационное сообщение**. Лицензия больше не действует для N устройств. • **Предупреждение**. Одно из следующих: M устройств с установленными приложениями "Лаборатории Касперского" на N устройствах в группах Сервера администрирования (N > M). Срок действия лицензии L истекает на N устройствах через M дней. Задача T по установке приложений успешно завершена на N устройствах, для M устройств требуется перезагрузка. • **Критический**. Срок действия лицензии истек для N устройств. • **OK**. Ничего из вышеперечисленного.
`noAntivirusSoftware`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.1	`deploymentStatus` – показывает, что в группах Сервера администрирования слишком много устройств, на которых не установлены управляемые приложения. Значение равно 1, если обнаружено нескольких устройств без управляемых приложений, и 0 в другом случае.
`remoteInstallTaskFailed`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.2	`deploymentStatus` – показывает, что на некоторых устройствах не удалось выполнить задачу удаленной установки. Количество этих устройств можно получить с помощью `hostsRemoteInstallFailed`.
`licenceExpiring`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.3	`deploymentStatus` – показывает, что есть несколько устройств, у которых истекает срок действия лицензии через семь дней. Количество этих устройств можно получить с помощью `hostsLicenseExpiring`.
`licenceExpired`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.4	`deploymentStatus` – показывает, что есть несколько устройств, у которых срок действия лицензии истек. Вы можете узнать количество этих устройств с помощью `hostsLicenseExpired`.

Значение идентификатора объекта	Числовой тип данных	OID	Описание
hostsInGroups	Counter32	.1.3.6.1.4.1.23668.1093.1.1.3	Количество устройств в группах Сервера администрирования.
hostsWithAntivirus	Counter32	.1.3.6.1.4.1.23668.1093.1.1.4	Количество устройств в группах Сервера администрирования с установленными управляемыми приложениями.
hostsRemoteInstallFailed	Counter32	.1.3.6.1.4.1.23668.1093.1.1.5	Количество устройств, на которых не удалось выполнить задачу удаленной установки.
licenceExpiringSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.6	Идентификатор лицензионного ключа, срок действия которого истечет менее чем через семь дней.
licenceExpiredSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.7	Идентификатор лицензионного ключа, срок действия которого истек.
licenceExpiringDays	Unsigned32	.1.3.6.1.4.1.23668.1093.1.1.8	Количество дней до истечения срока действия лицензии. Для этого параметра срок действия лицензии истек, если до истечения срока его действия осталось менее 7 дней. Если до истечения срока действия осталось более 7 дней, значение равно 0.
hostsLicenceExpiring	Counter32	.1.3.6.1.4.1.23668.1093.1.1.9	Количество устройств с лицензией, срок действия которой истекает менее чем через семь дней.
hostsLicenceExpired	Counter32	.1.3.6.1.4.1.23668.1093.1.1.10	Количество устройств, у которых истек срок действия лицензии.
updatesStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.2.1	Состояние обновления антивирусных баз. Статус может принимать одно из следующих значений: • **Информационное сообщение**. Антивирусные базы на Сервере администрирования или на устройствах не обновлялись более одного дня; с момента установки приложения прошло менее одного дня. • **Предупреждение**. Антивирусные базы на Сервере администрирования или на устройствах не обновлялись более 3 дней. Это значение можно изменить в свойствах группы. • **Критический**. Антивирусные базы на Сервере администрирования или на устройствах не обновлялись более 7 дней. Это значение можно изменить в свойствах группы. • **OK**. Ничего из вышеперечисленного.
serverNotUpdated	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.1	Давно не выполнялась полная проверка Сервера администрирования. Время, которое считается долгим, указывается в updatesStatus.
notUpdatedHosts	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.2	Некоторые устройства не обновлялись в течение долгого времени (по умолчанию **Критическое** – семь дней и более, **Предупреждение** – три дня). Вы можете узнать количество этих устройств с помощью hostsNotUpdated.
lastServerUpdateTime	Hex-STRING	.1.3.6.1.4.1.23668.1093.1.2.3	Дата последнего обновления антивирусных баз на Сервере администрирования.
hostsNotUpdated	Counter32	.1.3.6.1.4.1.23668.1093.1.2.4	Количество устройств, содержащих антивирусные базы, которые давно не обновлялись (по умолчанию **Критическое** – семь дней и более, **Предупреждение** – три дня). Если есть устройства со статусом обновления **Критическое**, учитываются только эти устройства. Вы можете получить статус обновления с помощью updatesStatus.

Значение идентификатора объекта	Числовой тип данных	OID	Описание
protectionStatus	INTEGER { ok(0), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.3.1	Статус постоянной защиты. Одно из следующих: • **Предупреждение**. Одно из следующих: На устройстве, входящем в группу Сервера администрирования, обнаружено нарушение безопасности. Из-за ошибок шифрования некоторые устройства изменили состояние защиты. Полная проверка давно не выполнялась. • **Критический**. На некоторых устройствах в группах Сервера администрирования не работает антивирусная защита. • **OK**. Ничего из вышеперечисленного.
antivirusNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.1	Приложение безопасности не работает на некоторых устройствах. Вы можете узнать количество этих устройств с помощью hostsAntivirusNotRunning.
realtimeNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.2	Постоянная защита не работает на некоторых устройствах. Вы можете узнать количество этих устройств с помощью hostsRealtimeNotRunning.
psRealtimeLevelChanged	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.3	Уровень защиты во время выполнения отличается от уровня, установленного администратором на N устройствах в группах администрирования.
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.4	Есть устройства с не вылеченными объектами. Вы можете узнать количество этих устройств с помощью hostsNotCuredObject.
tooManyThreats	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.5	Есть устройствах, на которых обнаружены угрозы. Вы можете узнать количество этих устройств с помощью hostsTooManyThreats.
virusOutbreak	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.6	Статус вирусной атаки системы. Значение равно 1, если определенное количество вирусов было обнаружено в течение определенного времени, и 0 в других случаях. Количество вирусов и время указывается на Сервере администрирования с помощью параметра Virus outbreak.
psVulnerabilitiesFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.7	Обнаружены уязвимости.
psEncryptionFaultsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.8	Обнаружены ошибки шифрования, изменившие состояние защиты устройства.
psVulnerableHostsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.9	На некоторых устройствах обнаружены уязвимости.
psNotScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.10	Обнаружены устройства, на которых не выполнялась полная проверка в течение длительного времени.
psNagentsNotRunningUntilReboot	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.11	Обнаружены устройства, на которых Агент администрирования запускается только после перезагрузки.
hostsAntivirusNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.3	Количество устройств, на которых не запущены приложения безопасности.
hostsRealtimeNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.4	Количество устройств, на которых не запущена постоянная защита.
hostsRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.5	Количество устройств с недопустимым уровнем постоянной защиты.
hostsNotCuredObject	Counter32	.1.3.6.1.4.1.23668.1093.1.3.6	Количество устройств с не вылеченными объектами.
hostsTooManyThreats	Counter32	.1.3.6.1.4.1.23668.1093.1.3.7	Количество устройств, которые содержат угрозы.

Значение идентификатора объекта	Числовой тип данных	OID	Описание
fullscanStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.4.1	Статус полной проверки может быть одним из следующих: • **Информационное сообщение**. С момента установки приложения прошло менее 7 дней. • **Предупреждение**. Полная проверка не производилась более 7 дней с момента установки приложения. • **Критический**. Полная проверка не производилась более 14 дней с момента установки приложения. • **OK**. Ничего из вышеперечисленного.
notScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.4.2.1	Есть несколько устройств, на которых не выполнялась проверка в течение определенного времени. Вы можете узнать количество этих устройств с помощью hostsNotScannedLately. Время указывается в fullScanStatus.
hostsNotScannedLately	Counter32	.1.3.6.1.4.1.23668.1093.1.4.3	Количество устройств, на которых не выполнялась проверка в течение определенного времени. Время указывается в fullScanStatus.
logicalNetworkStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.5.1	Состояние логической сети Сервера администрирования. Одно из следующих: • **Предупреждение**. Если есть устройства со статусом Предупреждение, к которым нет доступа, или если есть устройства, которые не принадлежат ни к какой группе Сервера администрирования. • **Критический**. Если есть устройства, контроль над которыми потерян Сервером администрирования, или есть устройства со статусом Критический, к которым нет доступа. • **OK**. Ничего из вышеперечисленного.
notConnectedLongTime	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.1	Есть несколько устройств, которые в течение долгого времени не были подключены к Серверу администрирования (семь дней и более для устройства со статусом **Предупреждение** и четыре дня для устройства со статусом **Критический**). Вы можете узнать количество этих устройств с помощью hostsNotConnectedLongTime.
controlLost	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.2	Есть устройства, контроль над которыми потерян Сервером администрирования. Вы можете узнать количество этих устройств с помощью hostsControlLost.
hostsFound	Counter32	.1.3.6.1.4.1.23668.1093.1.5.3	Количество обнаруженных Сервером администрирования устройств, не входящих ни в одну группу Сервера администрирования.
groupsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.5.4	Количество групп Сервера администрирования.
hostsNotConnectedLongTime	Counter32	.1.3.6.1.4.1.23668.1093.1.5.5	Количество устройств, которые долгое время не подключались к Серверу администрирования. Время, которое считается долгим, указывается в notConnectedLongTime.
hostsControlLost	Counter32	.1.3.6.1.4.1.23668.1093.1.5.6	Количество устройств, которые не контролируются Сервером администрирования.

Значение идентификатора объекта	Числовой тип данных	OID	Описание
`eventsStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.6.1	Статус событий подсистемы может быть одним из следующих: • **Предупреждение**. Одно из следующих: Устройства групп Сервера администрирования давно не выполняли поиск обновлений Windows. Есть устройства с проблемами, связанные со статусом. • **Критический**. Одно из следующих: Хотя бы на одном устройстве произошло критическое событие. Хотя бы на одном устройстве произошло событие отказа функционирования. Есть событие неудачного завершения задачи хотя бы на одном устройстве. Устройства групп Сервера администрирования давно не выполняли поиск обновлений Windows. Есть устройства с проблемами, связанные со статусом. • **Информационное сообщение.** Одно из следующих: С момента последней полной антивирусной проверки на всех устройствах прошло меньше недели. Задачи удаленной установки выполнены и ни одно устройство не требует перезагрузки. Последнее обновление Сервера администрирования выполнялось меньше недели назад. Сервер администрирования давно не обновлялся, но в сейчас выполняется обновление. • **OK**. Ничего из вышеперечисленного.
`criticalEventOccured`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.6.2.1	`eventsStatus` – показывает, что на Сервере администрирования произошли критические события. Вы можете получить количество этих событий с помощью `criticalEventsCount`. Значение равно 1, если есть хотя бы одно критическое событие на любом устройстве, и 0 в другом случае.
`criticalEventsCount`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.6.3	Количество критических событий на Сервере администрирования.

Использование Kaspersky Security Center Linux по лицензии Kaspersky Security для бизнеса Профессиональный

Если вы приобрели лицензию Kaspersky Security для бизнеса Профессиональный в составе лицензии на EPP-программу и лицензии Kaspersky Security Center Linux, вы сможете использовать функциональность Kaspersky Security для бизнеса Профессиональный после выполнения первоначальной настройки.

Если вы приобрели лицензию на Kaspersky Security для бизнеса Профессиональный отдельно в качестве расширения ранее приобретенной лицензии после установки и активации приложений "Лаборатории Касперского" на устройствах, вам нужно повторно активировать Kaspersky Security Center Linux на устройствах с помощью нового кода активации или файла ключа в зависимости от способа приобретения лицензии Kaspersky Security для бизнеса Профессиональный. После этого вы можете выполнить первоначальную настройку.

Также вы можете использовать функциональность Kaspersky Security для бизнеса Профессиональный в тестовом режиме. Для этого вам нужно сначала добавить физический подчиненный Сервер администрирования, а затем активировать этот Сервер по пробной лицензии Kaspersky Security для бизнеса Профессиональный. Функциональность Kaspersky Security для бизнеса Профессиональный будет доступна на подчиненном Сервере в течение срока действия пробной лицензии.

После активации Сервера администрирования по лицензии Kaspersky Security для бизнеса Профессиональный и распространения лицензионного ключа на устройства, управляемые соответствующим Сервером администрирования, вы можете выполнить следующее:

- Реагировать на угрозы с помощью интеграции с Kaspersky Automated Security Awareness Platform, Kaspersky Threat Intelligence Portal Sandbox и Active Directory.
- Группировать алерты по атрибутам.

Дополнительную информацию о функциях, включенных в лицензию Kaspersky Security для бизнеса Профессиональный, см. в справке Kaspersky Endpoint Detection and Response Optimum.

Интеграции для реагирования на алерты

Если у вас есть лицензия Kaspersky Security для бизнеса Профессиональный, вы можете настроить интеграцию со следующими решениями для реагирования на угрозы:

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

Эти интеграции доступны, если вы активировали Сервер администрирования по лицензии Kaspersky Security для бизнеса Профессиональный.
Для выполнения действий по реагированию вам нужно распространить лицензионный ключ Kaspersky Security для бизнеса Профессиональный на управляемые приложения.
При использовании функциональности Kaspersky Security для бизнеса Профессиональный по пробной лицензии вам нужно сначала добавить физический подчиненный Сервер администрирования, активировать этот подчиненный Сервер администрирования по пробной лицензии и распространить лицензионный ключ на ваши устройства, управляемые этим Сервером администрирования.

Если у вас есть лицензии Kaspersky Next EDR Optimum, вам не нужно активировать приложения, установленные на ваших управляемых устройствах по лицензии Kaspersky Security для бизнеса Профессиональный. Вам нужно сделать это только для новых устройств (при их наличии).

Поскольку лицензия Kaspersky Security для бизнеса Профессиональный поддерживает мультитенантность, вы можете централизованно распространять лицензионный ключ на управляемые приложения. Автоматическое распространение лицензии на подчиненные и виртуальные Серверы администрирования не поддерживается.

Чтобы настроить интеграцию, у вас должны быть права **Чтение** и **Запись** для функциональной области **Общие функции: Интеграция приложения**.

Настройка интеграции с Active Directory для выполнения действий по реагированию

Интеграция с Active Directory позволяет выполнять действия по реагированию для пользователей Active Directory, затронутых или вовлеченных в алерт.

Чтобы настроить интеграцию с Active Directory для реагирования на алерты, вам нужно использовать Сервер администрирования Kaspersky Security Center Linux версии 15.4 или выше.

Интеграция с Active Directory для реагирования на алерты и параметры проверки контроллера домена Active Directory (адрес и учетные данные пользователя контроллера домена), который вы указываете при настройке опроса контроллера домена, это два разных параметра. Поскольку вам нужно убедиться, что у пользователя, для которого должно выполняться действие по реагированию, есть учетная запись Active Directory, требуется настроить обе интеграции: для проверки и для реагирования. Порядок не имеет значения.

Параметры интеграции не наследуются, а применяются только к Серверу администрирования (физическому или виртуальному), на котором вы настраиваете эти параметры.

Чтобы настроить интеграцию с Active Directory для реагирования на алерты:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Выполните одно из следующих действий:

   - Выберите раздел **Точки распространения**, нажмите на название нужной точки распространения и в открывшемся окне свойств выберите раздел **Active Directory**.
   - Выберите раздел **Реагирование через Active Directory**.

3. В правой панели включите переключатель **Интеграция с Active Directory**.

   Если вы захотите позже выключить интеграцию, вы можете сделать это только для всех соединений, выключив переключатель **Интеграция с Active Directory**. Выключить интеграцию для отдельного соединения невозможно. Вы можете удалить соединение.

   > Когда вы включаете или выключаете переключатель **Интеграция с Active Directory**, этот параметр применяется как для раздела **Реагирование через Active Directory** и для раздела **Точки распространения**.

4. Создайте соединение к контроллеру домена Active Directory, нажав на кнопку **Добавить**.

5. В открывшемся окне настройте следующие параметры для соединения:

   - **Адрес контроллера домена**

     Имя компьютера, например: `server.mycompany.com`.

     Вы можете указать несколько IP-адресов. Все контроллеры домена, IP-адреса которых вы указываете, должны принадлежать одному домену.

   - **Имя домена Active Directory**

     Полное доменное имя DNS, например: `mycompany.com`.

     Также вы можете указать SAM-имя или NetBIOS-имя, например: `mycompany`.

     Используйте строчные буквы. Если вы создаете несколько соединений для Сервера администрирования или точки распространения, укажите разные имена для каждого соединения.

     > Для выполнения действий по реагированию имя домена Active Directory, указанное в этом поле, должно совпадать с именем домена Active Directory, указанным в алерте.

   - **Учетная запись**

     Войдите в Active Directory под учетной записью с правами администратора, под которой будут выполняться действия по реагированию.

   - **Пароль**

     Пароль учетной записи Active Directory с правами администратора, под которой будут выполняться действия по реагированию.

6. Если вы хотите проверить статус соединения, нажмите на кнопку **Проверить подключение**.

   Если соединение установлено, отображается статус **Подключено**. Иначе отображается статус **Сбой** и сообщение об ошибке с контроллерами домена, к которым не удалось подключиться.

Вам нужно учитывать способ подключения к Active Directory: **с Linux-устройства или с Windows-устройства**

Подключение с Linux-устройства

По умолчанию при подключении и аутентификации к контроллеру домена с Linux-устройства используется следующая логика:

1. Сервер администрирования или точка распространения пытается подключиться к контроллеру домена через LDAPS.

   Выполняется строгая проверка сертификата LDAP-сервера.

2. Вы помещаете открытую часть сертификата контроллера домена в хранилище действительных сертификатов системы для проверки сертификата.

   Для доступа к цепочке сертификатов системы используется зависящий от операционной системы путь к центру сертификации (CA).

   Например:

   - /etc/ssl/certs/ca-certificates.crt – путь для операционных систем на базе Debian (Debian, Ubuntu, Astra).
   - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem – путь для CentOS или Red Hat.

3. Если не удается выполнить LDAPS-соединение, возникает ошибка и никакой другой протокол соединения использовать невозможно.

   В случае возникновения проблем с LDAPS вы можете обратиться в Службу технической поддержки "Лаборатории Касперского".

Если вы не хотите устанавливать сертификат в хранилище сертификатов системы, вы можете использовать флаг KLNAG_LDAP_SSL_CACERT, чтобы задать путь к сертификату контроллера домена. Для этого выполните команду:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

где `</path/to/domain-controller/cert>` – путь к открытой части сертификата контроллера домена.

Например, если путь равен `"/var/opt/kaspersky/ldap_cert.crt"`, команда будет иметь вид `klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

Подключение с Windows-устройства

При подключении и аутентификации к контроллеру домена с Windows-устройства параметры подключения определяются доменом.

Вам нужно только убедиться в следующем:

- LDAPS включен и порт 636 доступен на устройстве.
- Вы разрешаете подключения к контроллеру домена через сетевой экран или прокси-сервер.

7. Нажмите на кнопку **Сохранить**.

Окно закроется и соединение отобразится в списке соединений.

В таблице соединений можно выполнять следующие действия:

- Изменять параметры соединения.

  Для этого перейдите по ссылке с параметром **Адрес контроллера домена** для нужного соединения. В открывшемся окне измените нужные параметры и нажмите на кнопку **Сохранить**.

  Вы можете изменить только параметры **Учетная запись** и **Пароль**.

- Удалять подключения.

  Для этого установите флажок рядом с тем соединением, которое вы хотите удалить, в панели инструментов нажмите на кнопку **Удалить** и подтвердите удаление соединения.

Настройка интеграции с Kaspersky Automated Security Awareness Platform

Интеграция с Kaspersky Automated Security Awareness Platform (далее также KASAP) позволяет назначать учебные курсы KASAP для пользователей, связанных с алертами.

Параметры интеграции не наследуются, а применяются только к Серверу администрирования (физическому или виртуальному), на котором вы настраиваете эти параметры.

Перед настройкой интеграции в Kaspersky Security Center Web Console необходимо создать токен авторизации и получить URL для API-запросов в KASAP.

Чтобы настроить интеграцию с Kaspersky Automated Security Awareness Platform:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Выберите раздел **KASAP**.

3. В правой панели включите переключатель **Интеграция с KASAP**.

4. Укажите параметры, которые будут использоваться для подключения к KASAP:

   - **API-токен** – токен, который вы создали для доступа к KASAP Open API.
   - **Веб-адрес** – URL для API-запросов, которые вы получили при создании API-токена.

- **Использовать прокси-сервер** – переключатель, позволяющий использовать прокси-сервер при подключении к KASAP.

  По умолчанию переключатель выключен.

5. При необходимости проверьте указанные вами параметры, нажав на кнопку **Проверить соединение**.

   Отображается статус соединения.

6. Нажмите на кнопку **Сохранить**.

Интеграция с Kaspersky Automated Security Awareness Platform настроена.

После сохранения параметров интеграции KASAP вы можете просмотреть список обучающихся групп KASAP, нажав на кнопку **Просмотреть группы**.

При необходимости вы можете обновить список отображаемых групп, нажав на кнопку **Обновить группы**.

Открытый список невозможно скрыть. Если вы выключите переключатель **Интеграция с KASAP**, список групп KASAP не будет отображаться.

Настройка интеграции с Kaspersky Threat Intelligence Portal Sandbox

Интеграция с Kaspersky Threat Intelligence Portal (далее также Kaspersky TIP) позволяет запускать исполняемые файлы, перемещенные в раздел **Карантин**, с помощью Kaspersky Sandbox – безопасной среды, изолированной от вашей корпоративной сети.

Параметры интеграции не наследуются, а применяются только к Серверу администрирования (физическому или виртуальному), на котором вы настраиваете эти параметры.

Перед настройкой интеграции вам нужно получить токен авторизации для API-запросов на Kaspersky TIP.

Чтобы настроить интеграцию с Kaspersky TIP Sandbox:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Выберите **Kaspersky TIP**.

3. В правой панели включите переключатель **Интеграция**.

   Отобразятся параметры подключения к Kaspersky TIP.

   Если после настройки и сохранения параметров интеграции вы выключите переключатель **Интеграция**, параметры не удаляются, но выполнить действие по реагированию будет невозможно.

4. Нажмите кнопку **Добавить токен**, в открывшемся окне укажите токен, ранее полученный на Kaspersky TIP, а затем нажмите кнопку **Добавить**.

   API-токен добавлен.

5. Если вы хотите использовать прокси-сервер при подключении к Kaspersky TIP, включите переключатель **Использовать прокси-сервер**.

   По умолчанию переключатель выключен.

6. Нажмите на кнопку **Сохранить**.

Интеграция с Kaspersky TIP Sandbox будет настроена.

Теперь вы можете отправлять файлы из раздела **Карантин** в Kaspersky TIP Sandbox для анализа угроз. Максимальный размер файла составляет 100 МБ.

Поскольку лицензия Kaspersky Security для бизнеса Профессиональный поддерживает мультитенантность, файлы, помещенные в **Карантин**, делятся по тенантам. Это разделение на уровне тенантов также применяется при отправке файлов в Kaspersky TIP Sandbox и при просмотре результатов, если администратор использует выделенную учетную запись Kaspersky TIP и API-токен, связанный с каждым тенантом. Однако централизованное управление разделом **Карантин** для всех тенантов невозможно, так как в списке объектов помещенных на карантин не отображаются объекты в соответствии с иерархией Сервера.

Группировка алертов по атрибутам

Агрегирование алертов помогает идентифицировать алерты, которые могут быть связаны с одним и тем же инцидентом, что упрощает процесс расследования.

Чтобы включить функцию агрегирования алертов, вам нужно выполнить следующее:

- Включить подраздел **Алерты** в главном меню.
- Активировать Сервер администрирования по лицензии Kaspersky Security для бизнеса Профессиональный, а затем распространить лицензионный ключ Kaspersky Security для бизнеса Профессиональный на управляемые приложения.

  При использовании функциональности по пробной лицензии Kaspersky Security для бизнеса Профессиональный вам нужно сначала добавить физический подчиненный Сервер администрирования, а затем активировать этот Сервер по этой лицензии.

Если у вас есть лицензии Kaspersky Next EDR Optimum, вам не нужно активировать приложения, установленные на ваших управляемых устройствах по лицензии Kaspersky Security для бизнеса Профессиональный. Вам нужно выполнить это только для новых устройств, если они есть. Поскольку лицензия Kaspersky Security для бизнеса Профессиональный поддерживает мультитенантность, вы можете централизованно распространять лицензионный ключ среди управляемых приложений. Автоматическое распространение лицензии на подчиненные и виртуальные Серверы администрирования не поддерживается.

Вы можете агрегировать алерты по имени устройства, учетной записи или SHA256.

> Алерты объединяются по атрибуту, только если этот атрибут не пуст.

Алерты объединяются, если они имеют хотя бы один атрибут и возникают в течение 24 часов после любого другого алерта в группе.

Чтобы агрегировать алерты по атрибутам:

1. В главном окне приложения перейдите в раздел **Мониторинг → Алерты**.
2. Выполните одно из следующих действий:

   - Включите переключатель **Агрегация алертов** и выберите один или несколько атрибутов, по которым нужно агрегировать алерты:

     - **Имя устройства**
     - **Учетная запись**
     - **Хеш файла (SHA256)**

     По умолчанию выбраны атрибуты **Имя устройства** и **Учетная запись**.

   - Нажмите на значок параметров (⚙). В открывшейся панели **Параметры таблицы** перейдите на вкладку **Группировка**. Выберите **Идентификатор группы агрегации** и нажмите **Применить**.

   > Когда агрегация включена, алерты сортируются по параметру **Время события** от самого нового к самому старому. Дополнительные параметры сортировки не поддерживаются. Выбор другой группы параметров выключит агрегацию.

   В таблице отображаются алерты, сгруппированные по атрибутам. Неагрегированные алерты перечислены внизу таблицы.

> Каждый алерт назначается только одной группе после агрегирования.

Интеграция Kaspersky Security Center Web Console с другими решениями "Лаборатории Касперского"

В этом разделе описывается, как настроить доступ из Kaspersky Security Center Web Console к другому приложению "Лаборатории Касперского", например Kaspersky Managed Detection and Response. В этом разделе также описано как настроить экспорт в SIEM-системы.

Установка фонового соединения

Чтобы настроить взаимодействие Kaspersky Security Center Linux с другим приложением "Лаборатории Касперского" или решением, например, Kaspersky Managed Detection and Response (далее также MDR), вам необходимо установить межсервисное соединение между Kaspersky Security Center Web Console и Сервером администрирования. Вы можете установить это соединение, только если в вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области **Общие функции: Права пользователя**.

> Вы можете настроить взаимодействие только между Kaspersky Managed Detection and Response и версией Kaspersky Security Center для Windows.

Чтобы установить фоновое соединение:

1. В главном меню перейдите в раздел **Параметры → Интеграция**.
2. Выберите вкладку **Параметры прокси-сервера Web Console**.
3. В разделе **Интеграция** переключите переключатель установки фонового соединения в положение: **Фоновое соединение для интеграции Включено**.
4. В разделе **Включить фоновое соединение** нажмите на кнопку **ОК**.

Фоновое соединение между Kaspersky Security Center Web Console и Сервером администрирования установлено. Сервер администрирования создает учетную запись для фонового подключения, и эта учетная запись используется как служебная учетная запись для поддержания взаимодействия Kaspersky Security Center Linux с другим приложением или решением "Лаборатории Касперского". Имя этой учетной записи службы содержит префикс NWCSvcUser. Сервер администрирования автоматически меняет пароль учетной записи службы каждые 30 дней в целях безопасности. Вы не можете удалить учетную запись службы вручную. Сервер администрирования автоматически удаляет эту учетную запись при отключении межсервисного соединения. Сервер администрирования создает единую учетную запись службы для каждой Kaspersky Security Center Web Console и Консоли администрирования и назначает все учетные записи службы группе безопасности с именем ServiceNwcGroup. Сервер администрирования создает эту группу безопасности автоматически в процессе установки Kaspersky Security Center Linux. Вы не можете удалить эту группу безопасности вручную.

Настройка соединения с прокси-сервером

Чтобы настроить подключение через прокси-сервер для Kaspersky Security Center Web Console и веб-плагинов:

1. В главном окне приложения перейдите в раздел **Параметры** → **Интеграция**.
2. Выберите вкладку **Параметры прокси-сервера Web Console**.
3. Включите параметр **Использовать прокси-сервер**.
4. Укажите параметры подключения к прокси-серверу:
   - **Адрес прокси-сервера**.
   - **Номер порта**.
   - **Аутентификация на прокси-сервере**.
   - **Имя пользователя** (требуется, если включен параметр **Аутентификация на прокси-сервере**).
   - **Пароль** (требуется, если включен параметр **Аутентификация на прокси-сервере**).
5. Нажмите **Сохранить**, чтобы сохранить параметры подключения к прокси-серверу.

Если у вас есть иерархия Серверов администрирования, параметры подключения к прокси-серверу не передаются в приложения Web Console, которые управляют подчиненными Серверами администрирования. Вам нужно настроить подключение к прокси-серверу отдельно для каждого приложения Kaspersky Security Center Web Console.

Удаленная диагностика клиентских устройств

Вы можете использовать удаленную диагностику для удаленного выполнения следующих операций на клиентских устройствах на базе Windows и Linux:

- включения и выключения трассировки, изменения уровня трассировки и загрузки файла трассировки;
- загрузки системной информации и параметров приложения;
- загрузки журналов событий;
- создание файла дампа для приложения;
- запуска диагностики и загрузки результатов диагностики;
- запуск, остановка и перезапуск приложений.

Вы можете использовать журнал событий и диагностические отчеты, загруженные с клиентского устройства, для устранения неполадок самостоятельно. Также если вы обращаетесь в Службу технической поддержки "Лаборатории Касперского", специалист технической поддержки "Лаборатории Касперского" может попросить вас загрузить файлы трассировки, файлы дампа, журнал событий и диагностические отчеты с клиентского устройства для дальнейшего анализа в "Лаборатории Касперского".

Открытие окна удаленной диагностики

Чтобы выполнить удаленную диагностику клиентских устройств на базе Windows и на базе Linux, сначала нужно открыть окно удаленной диагностики.

Чтобы открыть окно удаленной диагностики:

1. Чтобы выбрать устройство, для которого вы хотите открыть окно удаленной диагностики, выполните одно из следующих действий:
   - Если устройство принадлежит к группе администрирования, в главном меню перейдите в раздел **Управление активами** → **Управляемые устройства**.
   - Если устройство принадлежит к группе нераспределенных устройств, в главном меню перейдите в раздел **Управление активами** → **Нераспределенные устройства**.
2. Нажмите на имя требуемого устройства.
3. В открывшемся окне свойств устройства выберите вкладку **Дополнительно**.
4. На вкладке **Дополнительно** нажмите **Удаленная диагностика**.

   В результате открывается окно **Удаленная диагностика** клиентского устройства. Если отсутствует соединение между Сервером администрирования и клиентским устройством, появится сообщение об ошибке.

Если вам нужно получить сразу всю диагностическую информацию о клиентском устройстве с операционной системой Linux, вы можете запустить на этом устройстве скрипт collect.sh.

Включение и выключение трассировки для приложений

Вы можете включать и выключать трассировку для приложений, включая трассировку xperf.

Включение и выключение трассировки

Чтобы включить или выключить трассировку на удаленном устройстве:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В списке приложений выберите приложение, для которого требуется включить или выключить трассировку.

   Откроется список параметров удаленной диагностики.
4. Если вы хотите включить трассировку:

   a. В разделе **Трассировка** нажмите на кнопку **Включить трассировку**.

   b. В открывшемся окне **Изменить уровень трассировки** рекомендуется не менять значения, заданные по умолчанию. При необходимости специалист Службы технической поддержки проведет вас через процесс настройки. Доступны следующие параметры:

   - **Уровень трассировки**

     Уровень трассировки определяет состав информации, которую содержит файл трассировки.

   - **Трассировка на основе ротации**

     Приложение перезаписывает информацию трассировки, чтобы предотвратить чрезмерное увеличение файла трассировки. Укажите максимальное количество файлов, которые будут использоваться для хранения информации трассировки, и максимальный размер каждого файла. Если записано максимальное количество файлов трассировки максимального размера, самый старый файл трассировки будет удален, чтобы можно было записать новый файл трассировки.

     Этот параметр доступен только для Kaspersky Endpoint Security.

   c. Нажмите на кнопку **Сохранить**.

Трассировка включена для выбранного приложения. В некоторых случаях для включения трассировки приложения безопасности требуется перезапустить это приложение и его задачу.

На клиентских устройствах под управлением Linux трассировка компонента Обновление Агента администрирования регулируется параметрами Агента администрирования. Поэтому параметры **Включить трассировку** и **Изменить уровень трассировки** выключены для этого компонента на клиентских устройствах под управлением Linux.

5. Если вы хотите выключить трассировку для выбранного приложения, нажмите на кнопку **Выключить трассировку**.

   Трассировка выключена для выбранного приложения.

Включение трассировки Xperf

Для Kaspersky Endpoint Security специалисты Службы технической поддержки могут попросить вас включить трассировку Xperf для получения информации о производительности системы.

Чтобы включить, настроить или отключить трассировку Xperf:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.

3. В списке приложений выберите Kaspersky Endpoint Security для Windows.

   Откроется список параметров удаленной диагностики для Kaspersky Endpoint Security для Windows.

4. В разделе **Трассировка Xperf** нажмите на кнопку **Включить трассировку Xperf**.

   Если трассировка Xperf уже включена, отображается кнопка **Выключить трассировку Xperf**. Нажмите на эту кнопку, если хотите отключить трассировку Xperf для Kaspersky Endpoint Security для Windows.

5. В открывшемся окне **Изменить уровень трассировки Xperf**, в зависимости от запроса специалиста Службы технической поддержки, выполните следующее:

   a. Выберите один из уровней трассировки:

   - **Легкий уровень**

     Файл трассировки этого типа содержит минимальный объем информации о системе.

     По умолчанию выбран этот вариант.

   - **Детальный уровень**

     Файл трассировки этого типа содержит более подробную информацию, чем файл типа *Легкий уровень*, и может запрашиваться специалистами Технической поддержки, если информации в файле трассировки *легкого уровня* недостаточно для оценки производительности. Файл трассировки *Детального уровня* содержит информацию об оборудовании, операционной системе, список запущенных и завершенных процессов и приложений, событиях, используемых для оценки производительности, а также события Средства оценки системы Windows.

b. Выберите один из уровней трассировки Xperf:

- **Базовый тип**

  Приложение получает данные трассировки во время работы приложения Kaspersky Endpoint Security.

  По умолчанию выбран этот вариант.

- **Тип перезагрузки**

  Приложение получает данные трассировки, когда на управляемом устройстве запускается операционная система. Этот тип трассировки эффективен, когда проблема, влияющая на производительность системы, возникает после включения устройства и перед запуском Kaspersky Endpoint Security.

Также вам могут предложить включить параметр **Размер файлов ротации (МБ)**, чтобы предотвратить чрезмерное увеличение файла трассировки. Затем укажите максимальный размер файла трассировки. Когда файл достигает максимального размера, самый старый файл трассировки будет перезаписан новым файлом.

c. Определите размер файла ротации.

d. Нажмите на кнопку **Сохранить**.

Трассировка Xperf включена и настроена.

6. Если вы хотите отключить трассировку Xperf для Kaspersky Endpoint Security для Windows, нажмите **Выключить трассировку Xperf** в разделе **Трассировка Xperf**.

   Трассировка Xperf выключена.

Загрузка файла трассировки приложения

Чтобы загрузить файл трассировки приложения:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.

3. В списке приложений выберите приложение, для которого вы хотите загрузить файл трассировки.

4. В разделе **Трассировка** нажмите на кнопку **Файлы трассировки**.

   Откроется окно **Журналы удаленной установки**, где отображается список файлов трассировки.

5. В списке файлов трассировки выберите файл, который вы хотите загрузить.

6. Выполните одно из следующих действий:

   - Загрузите выбранный файл, нажав на кнопку **Скачать**. Вы можете выбрать один или несколько файлов для загрузки.

   - Загрузите часть выбранного файла:

     a. Нажмите на кнопку **Скачать часть**.

        Одновременная частичная загрузка нескольких файлов невозможна. Если вы выберете более одного файла трассировки, кнопка **Скачать часть** будет неактивна.

     b. В открывшемся окне укажите имя и часть файла для загрузки в соответствии с вашими требованиями.

        Для устройств под управлением Linux изменение имени части файла недоступно.

     c. Нажмите на кнопку **Скачать**.

Выбранный файл или его часть загружается в указанное вами расположение.

Удаление файлов трассировки

Вы можете удалить файлы трассировки, которые больше не нужны.

Чтобы удалить файл трассировки, выполните следующее действие:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В открывшемся окне удаленной диагностики выберите раздел **Журналы событий**.

3. В разделе **Файлы трассировки** нажмите **Журналы службы Центра обновления Windows** или **Журналы удаленной установки**, в зависимости от того, какие файлы трассировки вы хотите удалить.

   > Ссылка **Журналы службы Центра обновления Windows** доступна только для клиентских устройств под управлением Windows.

   Откроется окно **Журналы удаленной установки**, где отображается список файлов трассировки.

4. В списке файлов трассировки выберите один или несколько файлов, которые вы хотите удалить.

5. Нажмите на кнопку **Удалить**.

Выбранные файлы трассировки удалены.

Загрузка параметров приложений

Чтобы загрузить с клиентского устройства параметры приложений:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.
3. В разделе **Параметры приложения** нажмите на кнопку **Скачать** для загрузки информации о параметрах приложений, установленных на клиентском устройстве.

ZIP-архив с информацией загрузится в указанное расположение.

Загрузка системной информации с клиентского устройства

Чтобы загрузить системную информацию с клиентского устройства выполните следующие действия:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Информация о системе**.
3. Нажмите на кнопку **Скачать** для загрузки системной информации о клиентском устройстве.

   Если вы получаете системную информацию об устройстве под управлением Linux, в получившийся файл добавляется файл дампа для аварийно завершенных приложений.

   Архив может содержать конфиденциальные данные (например, ключи и пароли) в виде обычного текста. Рекомендуется просмотреть файлы в архиве и удалить такие данные перед отправкой в Службу технической поддержки "Лаборатории Касперского".

Файл с информацией загрузится в указанное расположение.

Загрузка журналов событий

Чтобы загрузить с удаленного устройства журнал событий:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В разделе **Журналы событий** в окне удаленной диагностики выберите **Все журналы устройства**.
3. В окне **Все журналы событий устройства** выберите один или несколько журналов событий.

4. Выполните одно из следующих действий:

   - Загрузите выбранный журнал событий, нажав на кнопку **Скачать весь файл**.
   - Загрузите часть выбранного журнала событий:

     a. Нажмите на кнопку **Скачать часть**.

     Одновременная частичная загрузка нескольких журналов событий невозможна. Если вы выберете более одного журнала событий, кнопка **Скачать часть** будет неактивна.

     b. В открывшемся окне укажите имя и часть журнала событий для загрузки в соответствии с вашими требованиями.

     Для устройств под управлением Linux изменение имени части журнала событий недоступно.

     c. Нажмите на кнопку **Скачать**.

Выбранный журнал событий или его часть загрузится в указанное расположение.

Запуск, остановка и перезапуск приложения

Вы можете запускать, останавливать и перезапускать приложения на клиентском устройстве.

Чтобы запустить, остановить или перезапустить приложение:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.

3. В списке приложений выберите приложение, которое вы хотите запустить, остановить или перезапустить.
4. Выберите действие, нажав на одну из следующих кнопок:

   - **Остановить приложение**

     Эта кнопка доступна, только если приложение в данный момент запущено.

   - **Перезапустить приложение**

     Эта кнопка доступна, только если приложение в данный момент запущено.

   - **Запустить приложение**

     Эта кнопка доступна, только если приложение в данный момент не запущено.

   В зависимости от выбранного вами действия требуемое приложение запустится, остановится или перезапустится на клиентском устройстве.

Если вы перезапустите Агент администрирования, появится сообщение о том, что текущее соединение устройства с Сервером администрирования будет потеряно.

Запуск удаленной диагностики Агента администрирования Kaspersky Security Center Linux и скачивание результатов

Чтобы запустить диагностику Агента администрирования Kaspersky Security Center Linux на удаленном устройстве и загрузить ее результаты:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В разделе списке приложений выберите **Агент администрирования Kaspersky Security Center Linux**.

   Откроется список параметров удаленной диагностики.
4. В разделе **Отчет диагностики** нажмите на кнопку **Выполнить диагностику**.

   Запускается процесс удаленной диагностики и генерируется отчет о диагностике. По завершении процесса диагностики кнопка **Скачать отчет диагностики** становится доступной.
5. Нажмите на кнопку **Скачать отчет диагностики**, чтобы загрузить отчет.

Отчет загрузится в указанное расположение.

Запуск приложения на клиентском устройстве

Вам может потребоваться запустить приложение на клиентском устройстве, если вас об этом попросит специалист Службы технической поддержки "Лаборатории Касперского". Вам не нужно устанавливать приложение самостоятельно на этом устройстве.

Если вы хотите запустить пользовательский скрипт на клиентском устройстве, вы можете использовать переменную среды `KLACDT_SAVE_SETTING`, чтобы определить путь, по которому будут сохранены результаты выполнения. Например:

- Для устройств с операционной системой Windows:

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```
- Для устройств с операционной системой Linux:

  ```
  echo some result > $KLACDT_SAVE_SETTING/res.log
  ```

Чтобы запустить приложение на клиентском устройстве:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Запуск удаленного приложения**.

3. В поле **Тип объекта** выберите тип объекта, который вы хотите загрузить:

   - Выберите **Файл** для загрузки исполняемого файла.
   - Выберите **Папка** для загрузки папки, содержащей приложение, которое вы хотите запустить на клиентском устройстве.

     Если вы выберете этот тип объекта, отобразится поле **Имя исполняемого файла, который будет запущен**. В этом поле укажите имя исполняемого файла в папке. Также можно указать относительный путь к файлу.
   - Выберите **Архив** для загрузки ZIP-архива, содержащего приложение, которое вы хотите запустить на клиентском устройстве.

     Если вы выберете этот тип объекта, отобразится поле **Имя исполняемого файла, который будет запущен**. В этом поле укажите имя исполняемого файла в папке. Также можно указать относительный путь к файлу.

     ZIP-архив должен содержать папку утилиты. Эта папка содержит исполняемый файл для запуска на удаленном устройстве.

4. Загрузите объект, выбрав его в системном окне или перетащив его в поле загрузки.
5. При необходимости в поле **Аргументы командной строки** укажите аргументы командной строки, которые будут переданы при запуске исполняемого файла.
6. Нажмите на кнопку **Загрузить и запустить** для запуска выбранного приложения на клиентском устройстве.
7. После успешного выполнения приложения, загрузите результаты выполнения, нажав на кнопку **Скачать результаты выполнения приложения**.

   Результаты выполнения приложения хранятся до тех пор, пока вы не запустите новую диагностику или не закроете окно.

Удаленная диагностика клиентского устройства с использованием приложения завершена.

Запуск удаленной диагностики на клиентском устройстве с операционной системой Linux

Kaspersky Security Center Linux позволяет загружать основную диагностическую информацию с клиентского устройства. Кроме того, вы можете получить диагностическую информацию об устройстве с операционной системой Linux с помощью скрипта collect.sh "Лаборатории Касперского". Этот скрипт запускается на клиентском устройстве с операционной системой Linux, которое необходимо диагностировать. Затем создается файл с диагностической информацией, системной информацией об этом устройстве, файлами трассировки приложений, журналами событий устройства и файлом дампа для аварийных ситуаций, прерванных приложений.

Рекомендуется использовать скрипт collect.sh для получения сразу всей диагностической информации о клиентском устройстве с операционной системой Linux. Если вы загружаете диагностическую информацию удаленно через Kaspersky Security Center Linux, вам нужно будет пройти все разделы интерфейса удаленной диагностики. Кроме того, диагностическая информация для устройства с операционной системой Linux, вероятно, не будет получена полностью.

Если вам необходимо отправить сформированный файл с диагностической информацией в Службу технической поддержки "Лаборатории Касперского", удалите всю конфиденциальную информацию перед отправкой файла.

Чтобы загрузить диагностическую информацию с клиентского устройства с операционной системой Linux с помощью скрипта collect.sh:

1. Загрузите скрипт collect.sh, который запакован в архив collect.tar.gz.
2. Скопируйте загруженный архив на клиентское устройство с операционной системой Linux, которое необходимо диагностировать.
3. Выполните следующую команду, чтобы распаковать архив collect.tar.gz:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Выполните следующую команду, чтобы указать права на выполнение скрипта:

   ```
   # chmod +x collect.sh
   ```

5. Запустите сценарий collect.sh под учетной записью с правами администратора:

   ```
   # ./collect.sh
   ```

Файл с диагностической информацией будет сформирован и сохранен в папке /tmp/$HOST_NAME-collect.tar.gz.

Управление сторонними приложениями и исполняемыми файлами на клиентских устройствах

В этом разделе описаны возможности Kaspersky Security Center Linux связанные с управлением сторонних приложений и исполняемых файлов на клиентских устройствах.

Использование компонента Контроль приложений для управления исполняемыми файлами

Вы можете использовать компонент Контроль приложений, чтобы разрешить или запретить запуск исполняемых файлов на пользовательских устройствах. Компонент Контроль приложений поддерживает операционные системы Windows и Linux.

> Для операционных систем Linux компонент Контроль приложений доступен, начиная с Kaspersky Endpoint Security 11.2 для Linux.

Предварительные требования

- Kaspersky Security Center Linux развернут в вашей организации.
- Политика Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Windows создана и активна. Компонент Контроль приложений включен в политике.

Этапы

Сценарий использования компонента Контроль приложений 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.

   Инструкции: Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах.

2. **Создание категорий для исполняемых файлов, используемых в вашей организации**

Проанализируйте списки исполняемых файлов, хранящихся на управляемых устройствах. На основе анализа сформируйте категории для исполняемых файлов. Рекомендуется создать категорию "Рабочие приложения", которая охватывает стандартный набор исполняемых файлов, используемых в вашей организации. Если разные группы безопасности используют свои наборы исполняемых файлов в своей работе, для каждой группы безопасности можно создать отдельную категорию.

Запуск исполняемых файлов, параметры которых не соответствуют ни одному из правил Контроля приложений, регулируется выбранным режимом работы компонента:

- *Список запрещенных*. Режим используется, если вы хотите разрешить запуск всех исполняемых файлов, кроме тех, которые указаны в запрещающих правилах. По умолчанию выбран этот режим.
- *Список разрешенных*. Режим используется, если вы хотите запретить запуск всех исполняемых файлов, кроме тех, которые указаны в разрешающих правилах.

Правила Контроля приложений реализованы в категориях для исполняемых файлов. В Kaspersky Security Center Linux существует три типа категорий исполняемых файлов:

- Пополняемая вручную категория. Вы определяете условия, например, метаданные файла, хеш файла, сертификат файла, путь к файлу, чтобы включить исполняемые файлы в категорию.
- Категория, в которую входят исполняемые файлы с выбранных устройств. Вы указываете устройство, исполняемые файлы которого автоматически включаются в категорию.
- Категория, в которую входят исполняемые файлы из выбранных папок. Вы указываете папку, исполняемые файлы из которой автоматически попадают в категорию.

3. **Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security**

   Настройте компонент Контроль приложений в политике Kaspersky Endpoint Security для Linux с использованием категорий, которые вы создали на предыдущем этапе.

   Инструкция: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows

4. **Включение компонента Контроль приложений в тестовом режиме**

   Чтобы правила Контроля приложений не блокировали исполняемые файлы, необходимые для работы пользователей, рекомендуется включить тестирование правил Контроля приложений и проанализировать их работу после создания правил. Когда тестирование включено, Kaspersky Endpoint Security для Windows не будет блокировать исполняемые файлы, запуск которых запрещен правилами Контроля приложений, а вместо этого будет отправлять уведомления об их запуске на Сервер администрирования.

   При тестировании правил Контроля приложений рекомендуется выполнить следующие действия:

   - Определите период тестирования. Период тестирования может варьироваться от нескольких дней до двух месяцев.
   - Изучите события, возникающие в результате тестирования работы компонента Контроль приложений.

   Инструкции для Kaspersky Security Center Web Console: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows. Следуйте этой инструкции и включите параметр **Тестовый режим** в процессе настройки.

5. **Изменение параметров компонента Контроль приложений**

   Если требуется, измените параметры компонента Контроль приложений. На основании результатов тестирования вы можете добавить исполняемые файлы, связанные с событиями компонента Контроль приложений, в категорию пополняемую вручную.

   Инструкции для Kaspersky Security Center Web Console: Добавление исполняемых файлов, связанных с событием, в категорию приложений.

6. **Применение правил Контроля приложений в рабочем режиме**

   После проверки правил Контроля приложений и завершения настройки категорий вы можете применить правила Контроль приложений в рабочем режиме.

   Инструкции для Kaspersky Security Center Web Console: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows. Следуйте этой инструкции и выключите параметр **Тестовый режим** в процессе настройки.

7. **Проверка конфигурации Контроля приложений**

   Убедитесь, что вы выполнили следующее:

   - Создали категории для исполняемых файлов.
   - Настроили Контроль приложений с использованием категорий.
   - Применили правила Контроля приложений в рабочем режиме.

Результаты

После завершения сценария, запуск исполняемых файлов на управляемых устройствах контролируется. Пользователи могут запускать только те исполняемые файлы, которые разрешены в вашей организации, и не могут запускать исполняемые файлы, запрещенные в вашей организации.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Windows.

Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах

Вы можете получить список исполняемых файлов, хранящихся на клиентских устройствах, одним из следующих способов:

- Включив уведомление о запуске приложений в политике Kaspersky Endpoint Security.
- Создав задачу инвентаризации.

Включение уведомлений о запуске приложений в политике Kaspersky Endpoint Security

Чтобы включить уведомления о запуске приложения:

1. Откройте параметры политики Kaspersky Endpoint Security и перейдите на вкладку **Общие параметры** → **Отчеты и хранилища**.
2. В группе параметров **Передача данных на Сервер администрирования** установите флажок **О запущенных приложениях** и сохраните изменения.

Когда пользователь пытается запустить исполняемые файлы, информация об этих файлах добавляется в список исполняемых файлов на клиентском устройстве. Kaspersky Endpoint Security отправляет эту информацию Агенту администрирования, а затем Агент администрирования отправляет ее на Сервер администрирования.

Создание задачи инвентаризации

Функция инвентаризации исполняемых файлов доступна для приложения Kaspersky Endpoint Security для Linux версии 11.2 и выше.

Вы можете снизить нагрузку на базу данных при получении информации об установленных приложениях. Для того чтобы сохранить место в базе данных, вам нужно запустить задачу инвентаризации на нескольких эталонных устройствах, на которых установлен стандартный набор приложений. Предпочтительное количество устройств равно 1–3.

Чтобы создать задачу инвентаризации исполняемых файлов на клиентских устройствах:

1. В главном окне приложения перейдите в раздел **Задачи**.

   Отобразится список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

3. На странице **Параметры новой задачи** в раскрывающемся списке **Приложение** выберите Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Windows в зависимости от типа операционной системы клиентских устройств.
4. В раскрывающемся списке **Тип задачи** выберите **Инвентаризация**.
5. На странице **Завершение создания задачи** нажмите на кнопку **Готово**.

   После того как мастер создания задачи завершит свою работу, задача **Инвентаризация** создана и настроена. Вы можете изменить параметры созданной задачи. В результате созданная задача отобразится в списке задач.

Подробное описание задачи инвентаризации см. в справке Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Windows.

После выполнения задачи **Инвентаризация** формируется список исполняемых файлов, хранящихся на управляемых устройствах, и вы можете просмотреть этот список.

Во время инвентаризации могут быть обнаружены исполняемые файлы в следующих форматах (в зависимости от выбранного вами параметра в свойствах задачи инвентаризации): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR и HTML.

Просмотр списка приложений и исполняемых файлов, хранящихся на управляемых устройствах

Чтобы просмотреть список исполняемых файлов, хранящихся на клиентских устройствах,

В главном окне приложения перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Исполняемые файлы**.

На странице отобразится список исполняемых файлов, хранящихся на клиентских устройствах.

При необходимости вы можете отправить исполняемый файл управляемого устройства на устройство, где открыто приложение Kaspersky Security Center Web Console.

Чтобы отправить исполняемый файл:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Исполняемые файлы**.
2. Перейдите по ссылке исполняемого файла, который вы хотите отправить.
3. В открывшемся окне перейдите в раздел **Устройства** и установите флажок рядом с управляемым устройством, с которого вы хотите отправить исполняемый файл.

   Перед отправкой исполняемого файла убедитесь, что управляемое устройство имеет прямое подключение к Серверу администрирования, установив флажок **Не разрывать соединение с Сервером администрирования**.

4. Нажмите на кнопку **Отправить**.

   Выбранный исполняемый файл будет загружен для дальнейшей отправки на устройство, на котором открыто приложение Kaspersky Security Center Web Console.

Создание пополняемой вручную категории приложений

Вы можете указать набор критериев в качестве шаблона для исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов, соответствующих критериям, вы можете создать категорию приложений и использовать ее в настройке компонента Контроль приложений.

Чтобы создать пополняемую вручную категорию приложений:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Категории приложений**.

   Откроется страница со списком категорий приложений.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге **Выбор способа создания категории**, укажите имя категории приложений и выберите параметр **Пополняемая вручную категория. Данные об исполняемых файлах добавляются в категорию вручную**.

4. На шаге **Условия** нажмите на кнопку **Добавить**, чтобы добавить критерий условия для включения файлов в создаваемую категорию.

5. На шаге **Критерии условия** выполните следующие действия:

   a. Выберите тип правила для создания категории:

   - **Из KL-категории**

     Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать категорию приложений "Лаборатории Касперского". Приложения, входящие в указанную KL-категорию, будут добавлены в пользовательскую категорию приложений.

   - **Выберите сертификат из хранилища сертификатов**

     Если выбран этот вариант, можно указать сертификаты из хранилища. Условие категории соответствует только исполняемым файлам, которые подписаны указанным сертификатом.

     Сертификаты будут добавлены в хранилище, если вы создали и запустили задачу инвентаризации или установили флажок **О запускаемых приложениях** в политике Kaspersky Endpoint Security. Вы можете выполнить оба действия.

     > Информация о сертификатах может быть извлечена только из исполняемых файлов формата PE (.exe, .dll, .sys).

   - **Задайте путь к приложению (поддерживаются маски)**

     Если выбран этот вариант, можно указать папку на клиентском устройстве, исполняемые файлы из которой будут добавлены в пользовательскую категорию приложений.

   - **Съемный диск**

     Если выбран этот вариант, можно указать тип носителя (любой или съемный диск), на котором выполняется запуск приложения. Приложения, запускаемые на носителе выбранного типа, будут добавлены в пользовательскую категорию приложений.

   - **Хеши файлов папки, метаданные файлов папки или сертификаты из папки**:

     - **Выберите из списка исполняемых файлов**

       Если выбран этот вариант, приложения для добавления в категорию можно выбрать из списка исполняемых файлов на клиентском устройстве.

     - **Выберите из реестра приложений**

Если выбран этот параметр, отображается реестр приложений. После того как вы выберете приложение из реестра, откроется окно с параметрами, заполненными метаданными из выбранного вами приложения:

- Имя файла.
- Версия файла. Вы можете указать точное значение версии или написать условие, например, "больше, чем 5.0".
- Название приложения.
- Версия приложения. Вы можете указать точное значение версии или написать условие, например, "больше, чем 5.0".
- Производитель.

Обратите внимание, что блокируется только запуск исполняемых файлов, соответствующих указанным параметрам, но не запуск выбранного вами приложения. Если выбранные метаданные приложения совпадают с метаданными исполняемого файла, который запускается при запуске приложения, вы можете перейти к следующему шагу. Иначе вам нужно будет изменить значения вручную, чтобы они совпадали с метаданными исполняемого файла.

- **Задайте вручную**

  Если выбран этот вариант, вам нужно указать хеш файла, метаданные или сертификат в качестве условия добавления приложений в пользовательскую категорию.

  Хеш файла

  В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky Security Center Linux для файлов категории. Информация о хеш-значениях, вычисленных хеш-функциями, хранится в базе данных Сервера администрирования.

  SHA256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security для Linux поддерживает вычисление SHA256.

  Выберите один из вариантов вычисления хеш-функции приложением Kaspersky Security Center Linux для файлов категории:

  - Если все экземпляры приложений безопасности, установленных в вашей сети, являются Kaspersky Endpoint Security для Linux, установите флажок **SHA256**.
  - Установите флажок **MD5-хеш**, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security для Linux не поддерживает хеш-функцию MD5.

  Метаданные

  Если этот параметр выбран, вы можете указать метаданные файла такие как имя файла, версию файла и поставщика. Условие категории соответствует только исполняемым файлам с одинаковыми метаданными.

  Сертификат

  Если выбран этот вариант, можно указать сертификаты из хранилища. Условие категории соответствует только исполняемым файлам, которые подписаны указанным сертификатом.

  Сертификаты будут добавлены в хранилище, если вы создали и запустили задачу инвентаризации или установили флажок **О запускаемых приложениях** в политике Kaspersky Endpoint Security. Вы можете выполнить оба действия.

- **Из архивной папки**

Если выбран этот параметр, вы можете указать файл в архивной папке и выбрать, какое условие вы хотите использовать для добавления приложений в пользовательскую категорию. Архивная папка распаковывается, и выбранные условия применяются к файлам в этой папке. В качестве условия, можно выбрать один следующих критериев:

- **Хеш файла**

  Вы можете выбрать, какую хеш-функцию (MD5 или SHA256) вы хотите использовать для вычисления значения хеш-функции. Приложения, имеющие такой же хеш, как и файлы в архивной папке, будут добавлены в пользовательскую категорию приложений.

  Выберите хеш-функцию MD5, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security для Linux не поддерживает хеш-функцию MD5.

- **Метаданные**

  Выберите, какие метаданные вы хотите использовать в качестве критерия. Исполняемые файлы, имеющие такие же метаданные, будут добавлены в пользовательскую категорию приложений.

- **Сертификат**

  Выберите, какие параметры сертификата (имя субъекта сертификата, отпечаток пальца или кем выписан сертификат) вы хотите использовать в качестве критерия. Исполняемые файлы, подписанные сертификатами, которые имеют те же параметры, будут добавлены в пользовательскую категорию.

Для использования критериев **Метаданные** и **Сертификат** нужно вручную указать их после загрузки файла или архивной папки.

Если выбран этот параметр, вы можете указать файл в архивной папке и выбрать, какое условие вы хотите использовать для добавления приложений в пользовательскую категорию. Архивная папка распаковывается, и выбранные условия применяются к файлам в этой папке. В качестве условия, можно выбрать один следующих критериев:

- **Хеш файла**

  Вы можете выбрать, какую хеш-функцию (MD5 или SHA256) вы хотите использовать для вычисления значения хеш-функции. Приложения, имеющие такой же хеш, как и файлы в архивной папке, будут добавлены в пользовательскую категорию приложений.

  Выберите хеш-функцию MD5, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security для Linux не поддерживает хеш-функцию MD5.

- **Метаданные**

  Выберите, какие метаданные вы хотите использовать в качестве критерия. Исполняемые файлы, имеющие такие же метаданные, будут добавлены в пользовательскую категорию приложений.

- **Сертификат**

  Выберите, какие параметры сертификата (имя субъекта сертификата, отпечаток пальца или кем выписан сертификат) вы хотите использовать в качестве критерия. Исполняемые файлы, подписанные сертификатами, которые имеют те же параметры, будут добавлены в пользовательскую категорию.

Для использования критериев **Метаданные** и **Сертификат** нужно вручную указать их после загрузки файла или архивной папки.

b. При необходимости добавьте комментарий в поле **Описание**. Количество символов не может превышать 1000.

Позже вы можете изменить или удалить комментарий. Для этого в свойствах категории приложений откройте вкладку **Условия**, а затем в столбце **Критерий условия** перейдите по ссылке с условием, для которого вы хотите изменить или удалить комментарий.

> При выборе типа правила **Из KL-категории** вы можете добавить один комментарий для всех условий, которые будут созданы на основе этого типа правила. Вы можете изменить или удалить комментарий для каждого условия отдельно.

Выбранный критерий добавлен в список условий.

Вы можете добавить любое количество критериев для создаваемой категории приложений.

6. На шаге **Исключения** нажмите на кнопку **Добавить**, чтобы добавить критерий в область исключений и исключить файлы из создаваемой категории.

   При необходимости вы можете добавите комментарий в поле **Описание**. Количество символов не может превышать 1000.

   Позже вы можете изменить или удалить комментарий. Для этого в свойствах категории приложений откройте вкладку **Исключения**, а затем в столбце **Критерий условия** перейдите по ссылке с условием, для которого вы хотите изменить или удалить комментарий.

7. На шаге **Критерии условия**, выберите тип правила из списка, так же, как вы выбрали тип правила для создания категории.

После завершения работы мастера категория приложений будет создана и отобразится в списке категорий приложений. Вы можете создать категорию приложений при настройке компонента Контроль приложений.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Windows.

Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств

Вы можете использовать исполняемые файлы с устройства как шаблон исполняемых файлов, запуск которых вы хотите разрешить или запретить. На основе исполняемых файлов с выбранных устройств вы можете создать категорию приложений и использовать ее для настройки компонента Контроль приложений.

Убедитесь, что выполнены следующие предварительные требования:

- Компонент Контроль приложений включен в политике Kaspersky Endpoint Security.
- Получен список исполняемых файлов, хранящихся на управляемых устройствах.

Чтобы создать категорию приложений, в которую входят исполняемые файлы с выбранных устройств:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Категории приложений**.

   Откроется страница со списком категорий исполняемых файлов.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге **Выбор способа создания категории** укажите имя категории и выберите параметр **Категория, в которую входят исполняемые файлы с выбранных устройств. Исполняемые файлы обрабатываются автоматически, их метрики заносятся в категорию**.

4. Нажмите на кнопку **Добавить**.

5. В открывшемся окне выберите устройство или устройства, чьи исполняемые файлы будут использоваться для создания категории приложений.

6. Задайте следующие параметры:

   - **Алгоритм вычисления хеш-функции**

     В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky Security Center Linux для файлов категории. Информация о хеш-значениях, вычисленных хеш-функциями, хранится в базе данных Сервера администрирования.

     SHA256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security для Linux поддерживает вычисление SHA256.

     Выберите один из вариантов вычисления хеш-функции приложением Kaspersky Security Center Linux для файлов категории:

     - Если все экземпляры приложений безопасности, установленных в вашей сети, являются Kaspersky Endpoint Security для Linux, установите флажок **SHA256**.

     Установите флажок **MD5-хеш**, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security для Linux не поддерживает хеш-функцию MD5.

     По умолчанию флажок **Вычислять SHA256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)** установлен.

     По умолчанию флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)** снят.

   - **Синхронизировать данные с хранилищем Сервера администрирования**

     Выберите этот параметр, если вы хотите, чтобы Сервер администрирования периодически выполнял проверку изменений в указанной папке (или папках).

     По умолчанию параметр выключен.

     Если вы включите этот параметр, укажите период (в часах), чтобы проверять изменения в указанной папке (папках). По умолчанию период проверки равен 24 часам.

   - **Тип файла**

     В этом разделе вы можете указать тип файла, который используется для создания категории приложений.

     Все файлы. Для создаваемой категории учитываются все файлы. По умолчанию выбран этот вариант.

     Только файлы вне категорий приложений. Для создаваемой категории учитываются только файлы вне категорий приложений.

- **Папки**

  В этом разделе вы можете указать папки выбранных устройств, содержащие файлы, которые используются для создания категории приложений.

  Все папки. Для создаваемой категории учитываются все папки. По умолчанию выбран этот вариант.

  Указанная папка. Для создаваемой категории учитывается только указанная папка. Если вы выбирали этот параметр, вам нужно указать путь к папке.

По завершении работы мастера создается категория исполняемых файлов. Она появится в списке категорий. Вы можете создать категорию при настройке компонента Контроль приложений.

Создание категории приложений, в которую входят исполняемые файлы из выбранных папок

Вы можете использовать исполняемые файлы выбранных папок как эталонный набор исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов из выбранных папок вы можете создать категорию приложений и использовать ее для настройки компонента Контроль приложений.

Чтобы создать категорию, в которую входят исполняемые файлы из выбранных папок:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Категории приложений**.

   Откроется страница со списком категорий.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге **Выбор способа создания категории**, укажите имя категории и выберите параметр **Категория, в которую входят исполняемые файлы из указанной папки. Исполняемые файлы приложений, копируемых в указанную папку, обрабатываются автоматически, и их метрики заносятся в категорию**.

4. Укажите папку, исполняемые файлы которой будут использоваться для создания категории.

5. Настройте следующие параметры:

   - **Включать в категорию динамически подключаемые библиотеки (DLL)**

     В категорию приложений включаются динамически подключаемые библиотеки (файлы формата DLL), и компонент Контроль приложений регистрирует действия таких библиотек, запущенных в системе. При включении файлов формата DLL в категорию возможно снижение производительности работы Kaspersky Security Center Linux.

     По умолчанию флажок снят.

   - **Включать в категорию данные о скриптах**

     В категорию приложений включаются данные о скриптах, и скрипты не блокируются компонентом Защита от веб-угроз. При включении данных о скриптах в категорию возможно снижение производительности работы Kaspersky Security Center Linux.

     По умолчанию флажок снят.

- **Алгоритм вычисления хеш-функции**: **Вычислять SHA256 для файлов в этой категории** / **Вычислять хеши MD5 для файлов в этой категории**

  В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky Security Center Linux для файлов категории. Информация о хеш-значениях, вычисленных хеш-функциями, хранится в базе данных Сервера администрирования.

  SHA256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security для Linux поддерживает вычисление SHA256.

  Выберите один из вариантов вычисления хеш-функции приложением Kaspersky Security Center Linux для файлов категории:

  - Если все экземпляры приложений безопасности, установленных в вашей сети, являются Kaspersky Endpoint Security для Linux, установите флажок **SHA256**.

  Установите флажок **MD5-хеш**, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security для Linux не поддерживает хеш-функцию MD5.

  По умолчанию флажок **Вычислять SHA256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)** установлен.

  По умолчанию флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)** снят.

- **Принудительно проверять папку на наличие изменений**

  Если этот параметр включен, приложение периодически принудительно проверяет папку пополнения категорий на наличие изменений. Периодичность проверки в часах можно указать в поле ввода рядом с флажком. По умолчанию период принудительной проверки равен 24 часам.

  Если этот параметр выключен, принудительная проверка папки не выполняется. Сервер обращается к файлам в папке в случае их изменения, добавления или удаления.

  По умолчанию параметр выключен.

По завершении работы мастера создается категория исполняемых файлов. Она появится в списке категорий. Вы можете использовать категорию для настройки компонента Контроль приложений.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Windows.

Просмотр списка категорий приложений

Вы можете просмотреть список настроенных категорий исполняемых файлов и параметры каждой категории.

Чтобы просмотреть список категорий приложений,

В главном окне приложения перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Категории приложений**.

Откроется страница со списком категорий.

Чтобы просмотреть свойства категории приложений,

нажмите на имя категории.

Откроется окно свойств выбранной категории. Параметры сгруппированы на нескольких вкладках.

Добавление исполняемых файлов, связанных с событием, в категорию приложения

После настройки компонента Контроль приложений в политиках Kaspersky Endpoint Security в списке событий могут отображаться следующие события:

- **Запуск приложения запрещен** (*Критическое* событие). Это событие отображается, если вы настроили Контроль приложений для применения правил.
- **Запуск приложения запрещен в тестовом режиме** (*Информационное* событие). Это событие отображается, если вы настроили Контроль приложений для применения правил в тестовом режиме.
- **Сообщение администратору о запрете запуска приложения** (сообщение с уровнем важности *Предупреждение*). Это событие отображается, если вы настроили Контроль приложений для применения правил, а пользователь запросил доступ к приложению, которое заблокировано для запуска.

Рекомендуется создавать выборки событий для просмотра событий, связанных с компонентом Контроль приложений.

Вы можете добавить исполняемые файлы, связанные с событиями Контроля приложений, в существующую категорию приложений или в новую категорию приложений. Вы можете добавлять исполняемые файлы только в категорию приложений пополняемую вручную.

Чтобы добавить исполняемые файлы, связанные с событиями компонента Контроль приложений, в категорию приложений:

1. В главном окне приложения перейдите в раздел **Мониторинг → Выборки событий**.

   Отобразится список выборок событий.

2. Выберите выборку событий, чтобы просмотреть события, связанные с Контролем приложений, и запустите формирование этой выборки событий.

   Если вы не создали выборку событий, связанную с Контролем приложений, вы можете выбрать и запустить предопределенную выборку, например, **Последние события**.

   Отобразится список событий.

3. Выберите события, связанные исполняемые файлы которых, вы хотите добавить в категорию приложений, и нажмите на кнопку **Назначить категорию**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. На странице мастера укажите необходимые параметры:

   - В разделе **Действие с исполняемым файлом, связанным с событием** выберите один из следующих вариантов:

     - **Добавить в новую категорию приложений**

       Выберите этот параметр, если вы хотите создать категорию приложений на основе исполняемых файлов, связанных с событиями.

       По умолчанию выбран этот вариант.

       Если вы выбрали этот параметр, укажите имя новой категории.

- **Добавить в существующую категорию**

  Выберите этот параметр, если вы хотите добавить исполняемые файлы, связанные с событиями, в существующую категорию приложений.

  По умолчанию вариант не выбран.

  Если вы выбрали этот параметр, выберите категорию приложений, пополняемую вручную, в которую вы хотите добавить исполняемые файлы.

- В разделе **Тип правила** выберите следующие параметры:

  - **Правила для добавления в область действия**

  - **Правила для добавления в исключения**

- В разделе **Параметр, используемый в качестве условия** выберите один из следующих вариантов:

  - **Данные сертификата (или SHA256 для файлов без сертификата)**

    Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одного приложения могут быть подписаны одним сертификатом или несколько разных приложений одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий приложения или несколько приложений одного производителя.

    Каждый файл имеет свою уникальную хеш-функцию SHA256. При выборе хеш-функции SHA256 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

    Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла или хеш-функцию SHA256 для файлов без сертификата.

    По умолчанию выбран этот вариант.

  - **Данные сертификата (файлы без сертификата пропускаются)**

    Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одного приложения могут быть подписаны одним сертификатом или несколько разных приложений одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий приложения или несколько приложений одного производителя.

    Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла. Если у исполняемого файла нет сертификата, то такой файл будет пропущен. Информация о нем не будет добавлена в категорию.

  - **Только SHA256 (файлы без хеша пропускаются)**

    Каждый файл имеет свою уникальную хеш-функцию SHA256. При выборе хеш-функции SHA256 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

    Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции SHA256 исполняемого файла.

  - **Только хеши MD5**

    > Выберите этот параметр, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security для Linux не поддерживает хеш-функцию MD5.

    Каждый файл имеет свою уникальную хеш-функцию MD5. При выборе хеш-функции MD5 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

5. Нажмите на кнопку **OK**.

   После завершения работы мастера исполняемые файлы, связанные с событиями Контроля приложений, добавляются в существующую категорию приложений или в новую категорию приложений. Вы можете просмотреть параметры категории приложений, которую вы изменили или создали.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Windows.

Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows

После создания категорий для Контроля приложений, вы можете использовать их для настройки Контроля приложений в политиках Kaspersky Endpoint Security для Windows.

Чтобы настроить компонент Контроль приложений в политике Kaspersky Endpoint Security для Windows:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

   Отобразится страница со списком политик.

2. Нажмите на политику **Kaspersky Endpoint Security для Windows**.

   Откроется окно свойств политики.

3. Перейдите в раздел **Параметры приложения** → **Контроль безопасности** → **Контроль приложений**.

   Отобразится окно **Контроль приложений** с параметрами компонента Контроль приложений.

4. Параметр **Контроль приложений** включен по умолчанию. Выключите переключатель **Контроль приложений [Выключен]**, чтобы выключить параметр.

5. В блоке **Параметры Контроля приложений** включите режим работы с применением правил Контроля приложений и разрешите Kaspersky Endpoint Security для Windows блокировку запуска приложений.

   Если вы хотите протестировать правила Контроля приложений, в разделе **Параметры Контроля приложений**, включите тестовый режим. В тестовом режиме Kaspersky Endpoint Security для Windows не блокирует запуск приложений, но фиксирует информацию о сработавших правилах в отчете. Перейдите по ссылке **Просмотреть отчет** для просмотра этой информации.

6. Включите параметр **Управление загрузкой модулей DLL**, если вы хотите, чтобы приложение Kaspersky Endpoint Security для Windows контролировало загрузку модулей DLL при запуске приложений пользователями.

   Информация о модуле и приложении, которое загрузило модуль, будет сохранена в отчете.

   Kaspersky Endpoint Security для Windows контролирует только DLL модули и драйверы, которые были загружены после того, как параметр **Управление загрузкой модулей DLL** был включен. Перезагрузите устройство после выбора параметра **Управление загрузкой модулей DLL**, если вы хотите, чтобы приложение Kaspersky Endpoint Security для Windows контролировало все модули и драйверы DLL, включая те, которые были загружены до запуска Kaspersky Endpoint Security для Windows.

7. (Если требуется.) В блоке **Шаблоны сообщений** измените шаблон сообщения, которое отображается, когда приложение заблокировано для запуска, и шаблон сообщения электронной почты, которое отправляется вам.

8. В блоке параметров **Режим Контроля приложений** выберите режим **Список запрещенных** или **Список разрешенных**.

   По умолчанию выбран режим **Список запрещенных**.

9. Перейдите по ссылке **Параметры списков правил**.

   Откроется окно **Списки запрещенных и разрешенных**, в котором можно добавить категорию приложений. По умолчанию отображается вкладка **Список запрещенных**, если выбран режим **Список запрещенных** или отображается вкладка **Список разрешенных**, если выбран режим **Список разрешенных**.

10. В окне **Списки запрещенных и разрешенных** нажмите на кнопку **Добавить**.

    Откроется окно **Правило Контроля приложений**.

11. Перейдите по ссылке **Пожалуйста, выберите категорию**.

    Откроется окно **Категории приложений**.

12. Добавьте категорию приложений (или категории), которые вы создали ранее.

    Вы можете изменить параметры категории, нажав на кнопку **Изменить**.

    Вы можете создать категорию, нажав на кнопку **Добавить**.

    Вы можете удалить категорию, нажав на кнопку **Удалить**.

13. После того как формирование списка категорий приложений завершено, нажмите на кнопку **OK**.

    Окно **Категории приложений** закрывается.

14. В окне правил **Контроль приложений** в разделе **Субъекты и их права** создайте список пользователей и групп пользователей, чтобы применить к ним правила Контроля приложений.

15. Нажмите на кнопку **OK**, чтобы сохранить параметры и закрыть окно **Правило Контроля приложений**.

16. Нажмите на кнопку **OK**, чтобы сохранить параметры и закрыть окно **Списки запрещенных и разрешенных**.

17. Нажмите на кнопку **OK**, чтобы сохранить параметры и закрыть окно **Контроль приложений**.

18. Закройте окно с параметрами политики Kaspersky Endpoint Security для Windows.

Компонент Контроль приложений настроен. После распространения политики на клиентские устройства запуск исполняемых файлов контролируется.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Windows.

Получение и просмотр списка приложений, установленных на клиентских устройствах

Kaspersky Security Center Linux выполняет инвентаризацию программного обеспечения, которое установлено на управляемых клиентских устройствах, работающих под управлением операционной системы Linux и Windows.

Агент администрирования составляет список приложений, установленных на устройстве, и передает список Серверу администрирования. Агенту администрирования требуется около 10–15 минут для обновления списка приложений.

Для клиентских устройств с операционной системой Windows Агент администрирования получает большую часть информации об установленных приложениях из реестра Windows. Для клиентских устройств с операционной системой Linux информацию об установленных приложениях Агент администрирования получает от диспетчеров пакетов.

Чтобы просмотреть список приложений, установленных на управляемых устройствах,

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Реестр приложений**.

   На странице отображается таблица с приложениями, установленными на управляемых устройствах. Выберите приложение, чтобы просмотреть свойства этого приложения, например: имя производителя, номер версии, список исполняемых файлов, список устройств, на которых установлено приложение.

2. Вы можете группировать и фильтровать данные таблицы с установленными приложениями следующим образом:

   - Нажмите на значок параметров ( ) в правом верхнем углу таблицы.

     В открывшемся меню **Параметры столбцов** выберите столбцы, которые будут отображаться в таблице. Чтобы просмотреть тип операционной системы клиентских устройств, на которых установлено приложение, выберите столбец **Тип ОС**.

   - Нажмите на значок фильтрации ( ) в правом верхнем углу таблицы, укажите и примените критерий фильтрации в открывшемся меню.

     Отобразится отфильтрованная таблица установленных приложений.

Чтобы просмотреть список приложений, установленных на выбранном управляемом устройстве,

В главном окне приложения перейдите в раздел **Управление активами → Управляемые устройства → имя устройства → Дополнительно → Реестр приложений**. В этом меню можно экспортировать список приложений в файлы форматов CSV или TXT.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Windows.

О приложениях сторонних производителей

Kaspersky Security Center Linux может помочь вам обновить приложения сторонних производителей, установленные на клиентских устройствах, и закрыть уязвимости в приложениях сторонних производителей. Kaspersky Security Center Linux может обновлять приложения сторонних производителей только с текущей версии до последней версии.

Список стороннего программного обеспечения обновляется динамически и может быть изменен. Вы можете проверить, возможно ли обновить приложения сторонних производителей, установленные на устройствах пользователей, с помощью Kaspersky Security Center Linux, просмотрев список доступных обновлений в Kaspersky Security Center Web Console.

Процедура ниже предназначена для просмотра списка стороннего программного обеспечения, которое можно обновить с помощью Kaspersky Security Center Linux. Для доступа к соответствующей информации без инициирования каких-либо задач необходимо выполнить описанные в процедуре действия.

Чтобы просмотреть список приложений сторонних производителей, которые можно обновить с помощью Kaspersky Security Center Linux:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. На шаге мастера **Параметры новой задачи** укажите следующие параметры:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Security Center Linux**.

   b. В поле **Тип задачи** выберите **Установка требуемых обновлений и закрытие уязвимостей**.
4. На шаге мастера **Область действия задачи** выберите параметр **Управляемые устройства**.
5. На шаге мастера **Задайте правила установки обновлений** нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.
6. На шаге мастера **Выбор типа правила** выберите параметр **Правило для сторонних обновлений**.
7. На шаге мастера **Общие критерии** выберите параметр **Устанавливать все обновления, кроме отклоненных** и нажмите на кнопку **Далее**.

Отобразится список приложений сторонних производителей.

Установка обновлений приложений сторонних производителей

Kaspersky Security Center Linux позволяет управлять обновлениями стороннего программного обеспечения, установленного на управляемых устройствах, и закрывать уязвимости в таких приложениях путем установки требуемых обновлений.

Kaspersky Security Center Linux выполняет поиск обновлений с помощью задачи *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Сервер администрирования получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, указанных в свойствах задачи и установленных на устройствах. После просмотра информации о доступных обновлениях вы можете выполнить установку обновлений на ваши устройства.

Обновление некоторых приложений Kaspersky Security Center Linux выполняет путем удаления предыдущей версии приложения и установки новой версии.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Из соображений безопасности любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных приложений с помощью технологий "Лаборатории Касперского". Эти технологии используются для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение.

Эксперты "Лаборатории Касперского" не проводят ручной анализ обновлений приложений сторонних производителей, которые можно установить с помощью Системного администрирования. Также эксперты "Лаборатории Касперского" не занимаются поиском уязвимостей (известных или неизвестных) или недокументированных возможностей в таких обновлениях и не проводят другие виды анализа упомянутых выше обновлений.

Когда метаданные обновлений стороннего программного обеспечения загружаются в хранилище, вы можете установить обновления на клиентские устройства, выполнив задачу *Установка требуемых обновлений и закрытие уязвимостей*.

> Задачу *Установка требуемых обновлений и закрытие уязвимостей* можно создать, только если у вас есть лицензия на Системное администрирование.

После завершения работы этой задачи обновления устанавливаются на управляемые устройства автоматически. При загрузке метаданных новых обновлений в хранилище Сервера администрирования Kaspersky Security Center Linux проверяет, соответствуют ли обновления критериям, указанным в правилах обновлений. Все новые обновления, которые соответствуют критериям, будут загружены и установлены автоматически при следующем запуске задачи.

Сценарий: обновление приложений сторонних производителей

В этом разделе представлен сценарий обновления приложений сторонних производителей, установленных на клиентских устройствах. Приложения сторонних производителей включают в себя приложения от других поставщиков программного обеспечения.

Предварительные требования

Сервер администрирования должен быть подключен к интернету для установки обновлений стороннего программного обеспечения.

Этапы

Обновление производителей состоит из следующих этапов:

1. **Поиск требуемых обновлений**

   Чтобы найти обновления приложений сторонних производителей, необходимые для управляемых устройств, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Kaspersky Security Center Linux получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, указанных в свойствах задачи и установленных на устройствах.

Задача *Поиск уязвимостей и требуемых обновлений* автоматически создается в Мастер первоначальной настройки Сервера администрирования. Если вы не запустили мастер, создайте задачу *Поиск уязвимостей и требуемых обновлений* или запустите мастер первоначальной настройки.

Вы можете создать задачу *Поиск уязвимостей и требуемых обновлений* только для устройств под управлением Windows. Вы не можете создать эту задачу для устройств, работающих под управлением других операционных систем.

2. **Просмотр списка найденных обновлений**

Просмотрите информацию о доступных обновлениях стороннего программного обеспечения и решите, какие обновления вы хотите установить. Чтобы просмотреть подробную информацию о каждом обновлении, нажмите на имя обновления в списке. Для каждого обновления в списке также можно просмотреть статистику установки обновлений на клиентских устройствах.

3. **Настройка установки обновлений**

После того как Kaspersky Security Center Linux получает список обновлений приложений сторонних производителей, вы можете установить их на клиентские устройства, создав задачу *Установка требуемых обновлений и закрытие уязвимостей*.

Вы можете создать задачу *Установка требуемых обновлений и закрытие уязвимостей* только для устройств под управлением Windows. Вы не можете создать эту задачу для устройств, работающих под управлением других операционных систем.

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для установки обновлений для приложений Microsoft, включая обновления, предоставляемые службой Центра обновления Windows, и обновления приложений других поставщиков. Обратите внимание, что задачу *Установка требуемых обновлений и закрытие уязвимостей* можно создать, только если у вас есть лицензия на Системное администрирование.

Для установки некоторых обновлений программного обеспечения вам нужно принять Лицензионное соглашение для установки программного обеспечения. Если вы отклоните Лицензионное соглашение, обновления программного обеспечения не будут установлены.

Вы можете запустить задачу установки обновления по расписанию. При указании расписания задачи убедитесь, что задача установки обновления запускается после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

4. **Задание расписания задачи**

Чтобы убедится, что список обновлений всегда актуален, задайте расписание запуска задачи *Поиск уязвимостей и требуемых обновлений*, чтобы она периодически запускалась автоматически. По умолчанию задача *Поиск уязвимостей и требуемых обновлений* настроена на запуск вручную.

Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете задать ее запуск с той же периодичностью, что и для задачи *Поиск уязвимостей и требуемых обновлений*, или реже.

При задании расписания задач убедитесь, что задача установки обновлений запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

5. **Одобрение и отклонение обновлений приложений сторонних производителей (необязательно)**

Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете указать правила установки обновлений в свойствах задачи.

Для каждого правила вы можете выбрать устанавливаемые обновления в зависимости от их статуса: *Не определено*, *Одобрено* или *Отклонено*. Например, вы можете создать определенную задачу для серверов и установить правило для этой задачи, чтобы разрешить установку только тех обновлений, которые имеют статус *Одобрено*. После этого вы вручную устанавливаете статус *Одобрено* для тех обновлений, которые вы хотите установить. В этом случае обновления со статусом *Не определено* или *Отклонено* не будут установлены на серверы, указанные в задаче.

При управлении установкой обновлений использовать статуса *Одобрено* целесообразно для небольшого количества обновлений. Чтобы установить несколько обновлений, используйте правила, которые вы можете настроить в задаче *Установка требуемых обновлений и закрытие уязвимостей*. Рекомендуется устанавливать статус *Одобрено* только для тех обновлений, которые не соответствуют критериям, указанным в правилах. Если вы подтверждаете вручную большое количество обновлений, производительность Сервера администрирования снижается, что может привести к перегрузке Сервера администрирования.

По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус на *Одобрено* или *Отклонено* в списке **Обновления ПО** (**Управление программным обеспечением** → **Управление патчами** → **Обновления ПО**).

Дополнительные сведения см. в инструкциях по одобрению и отклонению обновлений стороннего программного обеспечения.

6. **Запуск задачи установки обновлений**

   Запустите задачу *Установка требуемых обновлений и закрытие уязвимостей*. После запуска этой задачи, обновления загружаются и устанавливаются на управляемые устройства. После завершения задачи убедитесь, что в списке задач она имеет статус *Завершена успешно*.

7. **Создать отчет о результатах установки обновления (необязательно)**

   Чтобы просмотреть статистику установки обновления, сформируйте Отчет о результатах установки обновлений стороннего ПО.

Результаты

Если вы создали и настроили задачу *Установка требуемых обновлений и закрытие уязвимостей*, обновления будут автоматически установлены на управляемые устройства. При загрузке новых обновлений в хранилище Сервера администрирования Kaspersky Security Center Linux проверяет, соответствуют ли они критериям, указанным в правилах обновлений. Все новые обновления, которые соответствуют критериям, будут установлены автоматически при следующем запуске задачи.

Варианты установки обновлений стороннего программного обеспечения

Вы можете установить обновления стороннего программного обеспечения и обновления из Центра обновления Windows на управляемые устройства, создав и запустив задачу *Установка требуемых обновлений и закрытие уязвимостей*. Задачу *Установка требуемых обновлений и закрытие уязвимостей* можно создать, только если у вас есть лицензия на Системное администрирование. Вы можете использовать эту задачу для установки обновлений приложений сторонних производителей.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Также вы можете создать задачу для установки необходимых обновлений следующими способами:

- Открыть список обновлений и указать, какие обновления устанавливать.

  В результате создается задача для установки выбранных обновлений. Также вы можете добавить выбранные обновления в существующую задачу.

- Запустить мастер установки обновлений.

  Мастер установки обновления доступен при наличии лицензии на Системное администрирование.

  Мастер упрощает создание и настройку задачи установки обновлений и позволяет исключить создание избыточных задач, содержащих те же самые обновления для установки.

Установка обновлений приложений сторонних производителей с помощью списка обновлений

Чтобы установить обновления приложений сторонних производителей:

1. Откройте список обновлений, одним из следующих способов:

   - **Управление программным обеспечением** → **Управление патчами** → **Обновления ПО**.
   - **Управление активами** → **Управляемые устройства** → имя устройства → **Дополнительно** → **Применимые обновления**.
   - **Управление программным обеспечением** → **Сторонние приложения** → **Реестр приложений** → <имя приложения> → **Применимые обновления**.

   Отобразится список доступных обновлений.

2. Установите флажки рядом с теми обновлениями, которые вы хотите установить.

3. Нажмите на кнопку **Установить обновления**. Если эта кнопка не отображается, нажмите на кнопку с многоточием и в раскрывающемся списке выберите пункт **Установить обновления**.

   Для установки некоторых обновлений программного обеспечения вам нужно принять Лицензионное соглашение. Если вы отклоните Лицензионное соглашение, обновления программного обеспечения не установятся.

4. Выберите один из следующих вариантов:

   - **Новая задача**

     Запустится Мастер создания задачи. Если у вас есть лицензия на Системное администрирование, по умолчанию выбирается тип задачи *Установка требуемых обновлений и закрытие уязвимостей*. Следуйте далее указаниям мастера, чтобы завершить создание задачи.

   - **Установить обновление (добавить правило в указанную задачу)**

     Выберите задачу, в которую вы хотите добавить выбранные обновления. Если у вас есть лицензия на Системное администрирование, выберите задачу *Установка требуемых обновлений и закрытие уязвимостей*. В выбранную задачу автоматически добавлено правило для закрытия выбранных уязвимостей. Выбранные обновления добавлены в свойства задачи.

     Откроется окно свойств задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы выбрали создание задачи, она создается и отображается в списке задач в разделе **Задачи**. Если вы выбрали добавление обновлений в существующую задачу, обновления сохраняются в свойствах задачи.

Для установки обновлений стороннего программного обеспечения необходимо запустить задачу *Установка требуемых обновлений и закрытие уязвимостей*. Вы можете запустить эту задачу, нажав на кнопку **Запустить** в списке задач или указав параметры расписания в свойствах задачи, которую вы запускаете. При указании расписания задачи убедитесь, что задача установки обновления запускается после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

Установка обновлений приложений сторонних производителей с помощью мастера установки обновлений

Мастер установки обновления доступен при наличии лицензии на Системное администрирование.

Чтобы создать задачу установки обновлений приложений сторонних производителей с помощью мастера установки обновления:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Управление патчами** → **Обновления ПО**.

   Отобразится список доступных обновлений.

2. Установите флажок рядом с обновлением, которое вы хотите установить.

3. Нажмите на кнопку **Запустить мастер установки обновления**.

   Запустится мастер установки обновления. На странице **Выбор задачи установки обновления** отображается список всех существующих задач следующих типов:

   - *Установка требуемых обновлений и закрытие уязвимостей*
   - *Закрытие уязвимостей*

4. Если вы хотите, чтобы мастер отображал только те задачи, которые устанавливают выбранное вами обновление, включите параметр **Показать только задачи, которые устанавливают обновление**.

5. Выберите действие, которое хотите выполнить:

- Чтобы запустить существующую задачу, установите флажок рядом с задачей *Установка требуемых обновлений и закрытие уязвимостей* и нажмите на кнопку **Запустить**.

  Задача выполняется в фоновом режиме. Никаких дальнейших действий не требуется.

- Чтобы добавить новое правило в существующую задачу:

  a. Установите флажок рядом с именем задачи и нажмите на кнопку **Добавить правило**.

  > Кнопка **Добавить правило** недоступна, если вы выбрали более одной задачи.

  Вы не можете добавить правило для задачи *Закрытие уязвимостей*. Если вы выбрали задачу *Закрытие уязвимостей*, появится следующее уведомление: "*Для установки обновлений используйте задачу "Установка требуемых обновлений и закрытие уязвимостей"*".

  b. На шаге мастера **Создание правила установки обновления** настройте новое правило:

  - **Правило установки обновлений данного уровня важности**

    Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

    Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение важности выбранного обновления (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

    Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

    По умолчанию параметр выключен.

    Это правило не отображается, если уровень важности выбранного обновления – *Нет данных*.

  - **Правило установки обновлений данного уровня важности по MSRC**

    Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

    Если этот параметр включен (доступно только для обновлений Microsoft), обновления закрывают только те уязвимости, для которых уровень критичности, установленный Microsoft Security Response Center (MSRC), равен или превышает значение, выбранное в списке (**Низкий**, **Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

    Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

    По умолчанию параметр выключен.

    Это правило отображается только для обновлений программного обеспечения Microsoft. Правило не отображается, если уровень важности выбранного обновления – *Нет данных*.

  - **Правило установки обновлений данного поставщика**

Этот параметр доступен только для обновлений приложений сторонних производителей. Kaspersky Security Center Linux устанавливает только те обновления, которые относятся к приложениям того же производителя, что и выбранное обновление. Отклоненные обновления и обновления приложений других производителей не устанавливаются.

По умолчанию параметр выключен.

Это правило отображается только для обновлений стороннего программного обеспечения.

- **Правило установки обновлений типа**
- **Правило установки обновлений выбранного приложения**

  Это правило отображается только для обновлений стороннего программного обеспечения.

- **Правило установки выбранного обновления**
- **Одобрить выбранные обновления**

  Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

  По умолчанию параметр выключен.

- **Автоматически устанавливать все предыдущие обновления приложений, необходимые для установки выбранных обновлений**

  Включите этот параметр, если вы согласны с установкой промежуточных версий приложений, когда это необходимо, для установки выбранных обновлений.

  Если этот параметр выключен, устанавливаются только выбранные версии приложений. Выключите этот параметр, если вы хотите непосредственно обновить приложения, не пытаясь последовательно установить версии приложений. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

  Например, у вас на устройстве установлена версия 3 приложения, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

  По умолчанию параметр включен.

c. Нажмите на кнопку **Добавить**.

Откроется окно свойств задачи. Новое правило уже добавлено в свойства задачи. Вы можете просмотреть или изменить правило, а также другие параметры задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

- Чтобы создать задачу:

  a. Нажмите на кнопку **Новая задача**.

  b. На шаге мастера **Создание правила установки обновления** настройте новое правило:

  - **Правило установки обновлений данного уровня важности**

Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение важности выбранного обновления (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

Это правило не отображается, если уровень важности выбранного обновления – *Нет данных*.

- **Правило установки обновлений данного уровня важности по MSRC**

  Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

  Если этот параметр включен (доступно только для обновлений Microsoft), обновления закрывают только те уязвимости, для которых уровень критичности, установленный Microsoft Security Response Center (MSRC), равен или превышает значение, выбранное в списке (**Низкий**, **Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

  Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

  По умолчанию параметр выключен.

  Это правило отображается только для обновлений программного обеспечения Microsoft. Правило не отображается, если уровень важности выбранного обновления – *Нет данных*.

- **Правило установки обновлений данного поставщика**

  Этот параметр доступен только для обновлений приложений сторонних производителей. Kaspersky Security Center Linux устанавливает только те обновления, которые относятся к приложениям того же производителя, что и выбранное обновление. Отклоненные обновления и обновления приложений других производителей не устанавливаются.

  По умолчанию параметр выключен.

  Это правило отображается только для обновлений стороннего программного обеспечения.

- **Правило установки обновлений типа**

- **Правило установки обновлений выбранного приложения**

  Это правило отображается только для обновлений стороннего программного обеспечения.

- **Правило установки выбранного обновления**

- **Одобрить выбранные обновления**

  Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

  По умолчанию параметр выключен.

- **Автоматически устанавливать все предыдущие обновления приложений, необходимые для установки выбранных обновлений**

  Включите этот параметр, если вы согласны с установкой промежуточных версий приложений, когда это необходимо, для установки выбранных обновлений.

  Если этот параметр выключен, устанавливаются только выбранные версии приложений. Выключите этот параметр, если вы хотите непосредственно обновить приложения, не пытаясь последовательно установить версии приложений. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

  Например, у вас на устройстве установлена версия 3 приложения, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

  По умолчанию параметр включен.

c. Нажмите на кнопку **Добавить**.

Продолжите создавать задачу в мастере создания задачи. Новое правило, добавленное вами в мастере установки обновлений, отображается в мастере создания задачи. После завершения работы мастера задача *Установка требуемых обновлений и закрытие уязвимостей* добавлена в список задач.

Параметры задачи поиска уязвимостей и требуемых обновлений

Задача *Поиск уязвимостей и требуемых обновлений* создается автоматически во время работы мастера первоначальной настройки. Если вы не запускали мастер первоначальной настройки, вы можете создать задачу вручную.

Помимо общих параметров задачи, вы можете указать следующие параметры при создании задачи *Поиск уязвимостей и требуемых обновлений* или позже, при настройке свойств созданной задачи:

- **Поиск уязвимостей и обновлений, перечисленных Microsoft**

  При поиске уязвимостей и обновлений Kaspersky Security Center Linux использует данные о применимых обновлениях Microsoft из источника обновлений Microsoft, доступного в текущий момент.

  Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft и обновлений сторонних приложений.

  По умолчанию параметр включен.

  Информация о необязательных обновлениях Microsoft Windows не отправляется на Сервер администрирования.

- **Соединяться с сервером обновлений для актуализации данных**

  Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft. Следующие службы могут выступать в качестве источника обновлений Microsoft:

  - Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации.
  - Серверы обновления Microsoft.

Если этот параметр включен, Агент обновлений Windows на управляемом устройстве подключается к источнику обновлений Microsoft и получает информацию о применимых обновлениях Microsoft Windows.

Если этот параметр выключен, Агент обновлений Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, которую он получил из источника обновлений Microsoft ранее.

Подключение к источнику обновлений Microsoft может оказаться ресурсоемким. Вы можете выключить этот параметр, если у вас установлено регулярное подключение к этому источнику обновлений в другой задаче или в свойствах политики Агента администрирования, в разделе **Обновления и уязвимости в приложениях**. Если вы не хотите выключать этот параметр, то, чтобы уменьшить нагрузку на Сервер, вы можете настроить расписание задач так, чтобы использовать случайное значение задержки запуска задачи в интервале 360 минут.

По умолчанию параметр включен.

Комбинация следующих значений параметров политики Агента администрирования определяет режим получения обновлений:

- Агент обновлений Windows на управляемом устройстве подключается к серверу обновлений для получения обновлений только в случае, если параметр **Соединяться с сервером обновлений для актуализации данных** включен в свойствах задачи *Поиск уязвимостей и требуемых обновлений* и параметр **Режим поиска Центра обновления Windows** установлен в **Активный** в параметрах политики Агента администрирования.

- Если вам не требуется, чтобы Агент администрирования инициировал соединение с источником обновлений Microsoft Windows и загружал обновления при выполнении задачи *Поиск уязвимостей*, вы можете установить для параметра **Режим поиска Центра обновления Windows** значение **Пассивный**, при этом параметр **Соединяться с сервером обновлений для актуализации данных** должен оставаться включенным. Это позволяет сохранить ресурсы и использовать ранее полученные обновления Windows для поиска уязвимостей. Вы можете использовать пассивный режим, если настроили получение обновлений Microsoft Windows другим способом. Если получение обновлений Microsoft Windows не настроено по-другому, не устанавливайте для параметра **Режим поиска Центра обновления Windows** значение **Пассивный**, так как в этом случае информация об обновлениях никогда не будет получена.

- Независимо от параметра **Соединяться с сервером обновлений для актуализации данных** (включен он или выключен), если для параметра **Выключен** выбрано значение **Режим поиска Центра обновления Windows**, Kaspersky Security Center Linux не запрашивает информацию об обновлениях.

Если в сети вашей организации используется WSUS-сервер (локальный WSUS-сервер) и вы хотите использовать его вместе с Сервером администрирования Kaspersky Security Center, вам нужно сначала убедиться, что Сервер администрирования Kaspersky Security Center не используется в качестве WSUS-сервера, а затем выполнить следующие действия:

1. На управляемых устройствах с операционной системой Windows указать локальный WSUS-сервер для службы Центра обновления Windows. Вы можете сделать это вручную в реестре Windows или с помощью групповой политики Windows.

2. На локальном WSUS-сервере указать требуемые классификации для обновлений и приложений, по которым они будут распространяться.

3. Синхронизировать свой WSUS-сервер с вышестоящим сервером (это может быть либо Microsoft WSUS-сервер, либо другой локальный вышестоящий WSUS-сервер).

После запуска задачи *Поиск уязвимостей и требуемых обновлений* на устройстве Агент администрирования с помощью службы Центра обновления Windows инициирует запрос обновлений Windows, применимых к устройству. Служба Центра обновления Windows получает адрес внешнего WSUS-сервера из реестра и выполняет поиск обновлений непосредственно с этого внешнего WSUS-сервера. Затем служба Центра обновления Windows пересылает этот список на Сервер администрирования с помощью Агента администрирования. Таким образом, Сервер администрирования имеет актуальную базу.

- **Поиск уязвимостей и обновлений сторонних производителей, перечисленных "Лабораторией Касперского"**

  Если этот параметр включен, Kaspersky Security Center Linux выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите пути для дополнительного поиска приложений в файловой системе**. Полный список поддерживаемых приложений сторонних производителей контролируется "Лабораторией Касперского".

  Если этот параметр выключен, Kaspersky Security Center Linux не выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних приложений.

  По умолчанию параметр включен.

- **Укажите пути для дополнительного поиска приложений в файловой системе**

  Папки, в которых Kaspersky Security Center Linux выполняет поиск сторонних приложений, требующих закрытия уязвимостей и установки обновлений. Вы можете использовать системные переменные.

  Укажите папки, в которые были установлены приложения. По умолчанию список содержит системные папки, в которые устанавливается большинство приложений.

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать файлы трассировки, даже если запись файлов трассировки выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center Linux. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center Linux. Дополнительная трассировка не записывается.

  При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

  По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

  По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

Рекомендации по настройке расписания запуска задачи

При планировании расписания запуска задачи *Поиск уязвимостей и требуемых обновлений* убедитесь, что включены два параметра **Запускать пропущенные задачи** и **Использовать автоматическое определение случайного интервала между запусками задачи**.

По умолчанию задача *Поиск уязвимостей и требуемых обновлений* настроена на запуск вручную. Если регламент работы организации предусматривает выключение устройств в это время, то задача *Поиск уязвимостей и требуемых обновлений* будет запущена после включения устройства (утром следующего дня). Такое поведение может быть нежелательным, так как поиск уязвимостей может вызывать повышенную нагрузку на процессор и дисковую подсистему устройства. Следует настроить оптимальное расписание задачи исходя из принятого в организации регламента работы.

Создание задачи Поиск уязвимостей и требуемых обновлений

С помощью задачи *Поиск уязвимостей и требуемых обновлений* Kaspersky Security Center Linux получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, установленных на управляемых устройствах.

> Вы можете создать задачу *Поиск уязвимостей и требуемых обновлений* только для устройств под управлением Windows. Вы не можете создать эту задачу для устройств, работающих под управлением других операционных систем.

Задача *Поиск уязвимостей и требуемых обновлений* создается автоматически во время работы мастера первоначальной настройки. Если вы не запускали мастер первоначальной настройки, вы можете создать задачу вручную.

Чтобы создать задачу Поиск уязвимостей и требуемых обновлений:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится Мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для приложения Kaspersky Security Center выберите тип задачи **Поиск уязвимостей и требуемых обновлений**.
4. Укажите название задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите устройства, которым будет назначена задача.
6. Укажите способы проверки уязвимостей и приложений, требующих обновления:

   - **Поиск уязвимостей и обновлений, перечисленных Microsoft**

     При поиске уязвимостей и обновлений Kaspersky Security Center Linux использует данные о применимых обновлениях Microsoft из источника обновлений Microsoft, доступного в текущий момент.

Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft и обновлений сторонних приложений.

По умолчанию параметр включен.

Информация о необязательных обновлениях Microsoft Windows не отправляется на Сервер администрирования.

- **Соединяться с сервером обновлений для актуализации данных**

  Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft. Следующие службы могут выступать в качестве источника обновлений Microsoft:

  - Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации.
  - Серверы обновления Microsoft.

  Если этот параметр включен, Агент обновлений Windows на управляемом устройстве подключается к источнику обновлений Microsoft и получает информацию о применимых обновлениях Microsoft Windows.

  Если этот параметр выключен, Агент обновлений Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, которую он получил из источника обновлений Microsoft ранее.

  Подключение к источнику обновлений Microsoft может оказаться ресурсоемким. Вы можете выключить этот параметр, если у вас установлено регулярное подключение к этому источнику обновлений в другой задаче или в свойствах политики Агента администрирования, в разделе **Обновления и уязвимости в приложениях**. Если вы не хотите выключать этот параметр, то, чтобы уменьшить нагрузку на Сервер, вы можете настроить расписание задач так, чтобы использовать случайное значение задержки запуска задачи в интервале 360 минут.

  По умолчанию параметр включен.

Комбинация следующих значений параметров политики Агента администрирования определяет режим получения обновлений:

- Агент обновлений Windows на управляемом устройстве подключается к серверу обновлений для получения обновлений только в случае, если параметр **Соединяться с сервером обновлений для актуализации данных** включен в свойствах задачи *Поиск уязвимостей и требуемых обновлений* и параметр **Режим поиска Центра обновления Windows** установлен в **Активный** в параметрах политики Агента администрирования.

- Если вам не требуется, чтобы Агент администрирования инициировал соединение с источником обновлений Microsoft Windows и загружал обновления при выполнении задачи *Поиск уязвимостей*, вы можете установить для параметра **Режим поиска Центра обновления Windows** значение **Пассивный**, при этом параметр **Соединяться с сервером обновлений для актуализации данных** должен оставаться включенным. Это позволяет сохранить ресурсы и использовать ранее полученные обновления Windows для поиска уязвимостей. Вы можете использовать пассивный режим, если настроили получение обновлений Microsoft Windows другим способом. Если получение обновлений Microsoft Windows не настроено по-другому, не устанавливайте для параметра **Режим поиска Центра обновления Windows** значение **Пассивный**, так как в этом случае информация об обновлениях никогда не будет получена.

- Независимо от параметра **Соединяться с сервером обновлений для актуализации данных** (включен он или выключен), если для параметра **Выключен** выбрано значение **Режим поиска Центра обновления Windows**, Kaspersky Security Center Linux не запрашивает информацию об обновлениях.

Если в сети вашей организации используется WSUS-сервер (локальный WSUS-сервер) и вы хотите использовать его вместе с Сервером администрирования Kaspersky Security Center, вам нужно сначала убедиться, что Сервер администрирования Kaspersky Security Center не используется в качестве WSUS-сервера, а затем выполнить следующие действия:

1. На управляемых устройствах с операционной системой Windows указать локальный WSUS-сервер для службы Центра обновления Windows. Вы можете сделать это вручную в реестре Windows или с помощью групповой политики Windows.

2. На локальном WSUS-сервере указать требуемые классификации для обновлений и приложений, по которым они будут распространяться.

3. Синхронизировать свой WSUS-сервер с вышестоящим сервером (это может быть либо Microsoft WSUS-сервер, либо другой локальный вышестоящий WSUS-сервер).

После запуска задачи *Поиск уязвимостей и требуемых обновлений* на устройстве Агент администрирования с помощью службы Центра обновления Windows инициирует запрос обновлений Windows, применимых к устройству. Служба Центра обновления Windows получает адрес внешнего WSUS-сервера из реестра и выполняет поиск обновлений непосредственно с этого внешнего WSUS-сервера. Затем служба Центра обновления Windows пересылает этот список на Сервер администрирования с помощью Агента администрирования. Таким образом, Сервер администрирования имеет актуальную базу.

- **Поиск уязвимостей и обновлений сторонних производителей, перечисленных "Лабораторией Касперского"**

  Если этот параметр включен, Kaspersky Security Center Linux выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите пути для дополнительного поиска приложений в файловой системе**. Полный список поддерживаемых приложений сторонних производителей контролируется "Лабораторией Касперского".

Если этот параметр выключен, Kaspersky Security Center Linux не выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних приложений.

По умолчанию параметр включен.

Вы можете выключить эти параметры после создания задачи на вкладке **Параметры приложения** в окне свойств задачи.

7. **Укажите пути для дополнительного поиска приложений в файловой системе**

   Папки, в которых Kaspersky Security Center Linux выполняет поиск сторонних приложений, требующих закрытия уязвимостей и установки обновлений. Вы можете использовать системные переменные.

   Укажите папки, в которые были установлены приложения. По умолчанию список содержит системные папки, в которые устанавливается большинство приложений.

   Вы можете изменить указанные пути после создания задачи на вкладке **Параметры приложения** в окне свойств задачи.

8. При необходимости **Включить расширенную диагностику**

   Если этот параметр включен, Агент администрирования будет записывать файлы трассировки, даже если запись файлов трассировки выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center Linux. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

   Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center Linux. Дополнительная трассировка не записывается.

   При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

   По умолчанию параметр выключен.

   Вы можете выключить этот параметр после создания задачи на вкладке **Параметры приложения** в окне свойств задачи.

9. Укажите **Максимальный размер файлов расширенной диагностики, МБ**

   По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

   Вам нужно указать это значение, если вы включили расширенную диагностику на предыдущем шаге. Вы можете изменить это значение после создания задачи на вкладке **Параметры приложения** в окне свойств задачи.

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**.

    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 создана и настроена. Чтобы запустить задачу, выберите задачу в списке задач и нажмите на кнопку **Запустить**.

Рекомендации по настройке расписания запуска задачи

При планировании расписания запуска задачи *Поиск уязвимостей и требуемых обновлений* убедитесь, что включены два параметра **Запускать пропущенные задачи** и **Использовать автоматическое определение случайного интервала между запусками задачи**.

По умолчанию задача *Поиск уязвимостей и требуемых обновлений* настроена на запуск вручную.

Вы также можете настроить расписание запуска задачи *Поиск уязвимостей и требуемых обновлений* в определенное время. Например, вы можете выбрать запуск по расписанию **Каждый N час** из раскрывающегося списка **Запуск задачи** на вкладке **Расписание** окна свойств задачи. В этом случае, если регламент работы организации предусматривает выключение устройств в это время, то задача *Поиск уязвимостей и требуемых обновлений* будет запущена после включения устройства. Такое поведение может быть нежелательным, так как поиск уязвимостей может вызывать повышенную нагрузку на процессор и дисковую подсистему устройства. Следует настроить оптимальное расписание задачи исходя из принятого в организации регламента работы.

Подробное описание параметров запуска по расписанию см. в общих параметрах задачи.

Просмотр информации о доступных обновлениях приложений сторонних производителей.

Вы можете просмотреть список доступных обновлений для приложений сторонних производителей, включая программное обеспечение Microsoft, установленных на клиентских устройствах.

Чтобы просмотреть список доступных обновлений для приложений сторонних производителей, установленных на клиентских устройствах,

В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Управление патчами** → **Обновления ПО**.

Отобразится список доступных обновлений.

Вы можете указать фильтр для просмотра списка обновлений приложений. Нажмите на значок **Фильтр** () в списке обновлений приложений для управления фильтром. Вы также можете выбрать один из предустановленных фильтров в раскрывающемся списке **Предустановленные фильтры** над списком уязвимостей в приложениях.

Чтобы просмотреть свойства обновления:

1. Нажмите на имя требуемого обновления программного обеспечения.
2. Откроется окно свойств обновления, в котором отображается следующая информация, сгруппированная по вкладкам:

   - **Общие**

     На этой вкладке отображаются общие сведения о выбранном обновлении:

     - Статус одобрения обновления (можно изменить вручную, выбрав новый статус в раскрывающемся списке).
     - Дата и время регистрации обновления.
     - Дата и время создания обновления.
     - Уровень важности обновления.
     - Требования к установке, предъявляемые обновлением.
     - Семейство приложений, к которому относится обновление.
     - Приложение, к которому применяется обновление.
     - Номер версии обновления.

   - **Атрибуты**

     На этой вкладке отображается набор атрибутов, которые вы можете использовать для получения дополнительных сведений о выбранном обновлении. Этот набор различается в зависимости от того, кем выпущено обновление: Microsoft или сторонним производителем.

     На вкладке отображается следующая информация об обновлении Microsoft:

     - Уровень важности обновления в соответствии Microsoft Security Response Center (MSRC).
     - Ссылка на статью в базе знаний Microsoft с описанием обновления.
     - Ссылка на статью в бюллетене Microsoft Security Bulletin с описанием обновления.
     - Идентификатор обновления (ID).

     На вкладке отображается следующая информация для обновления стороннего производителя:

     - Является ли обновление патчем или полным дистрибутивом.
     - Язык локализации обновления.
     - Устанавливается ли обновление автоматически или вручную.
     - Было ли обновление отозвано после применения.
     - Ссылка для загрузки обновления.

- **Устройства**

  На этой вкладке отображается список устройств, на которых установлено выбранное обновление.

- **Закрываемые уязвимости**

  На этой вкладке отображается список уязвимостей, которые выбранное обновление может закрыть.

- **Пересечения обновлений**

  На этой вкладке отображаются возможные пересечения между различными обновлениями, опубликованными для одного и того же приложения, то есть может ли выбранное обновление заменять другие обновления или, наоборот, можно ли его заменять другими обновлениями (доступно только для обновлений Microsoft).

- **Задачи для установки обновления**

  На этой вкладке отображается список задач, в область действия которых входит установка выбранного обновления. На вкладке также можно создать задачу удаленной установки обновления.

Чтобы просмотреть статистику установки обновления:

1. Установите флажок рядом с требуемым обновлением.
2. Нажмите на кнопку **Статистика состояния установки обновлений**.

На диаграмме отобразится информация о статусах обновлений. При нажатии на статус открывается список устройств с выбранным статусом.

Вы можете просмотреть информацию о доступных обновлениях для приложений сторонних производителей, включая программное обеспечение Microsoft, установленных на выбранном управляемом устройстве под управлением Windows.

Чтобы просмотреть список доступных обновлений для приложений сторонних производителей, установленных на выбранном управляемом устройстве:

1. В главном окне приложения перейдите в раздел **Управление активами → Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием устройства, для которого вы хотите просмотреть обновления приложений сторонних производителей.

   Откроется окно свойств выбранного устройства.

3. В окне свойств выбранного устройства выберите вкладку **Дополнительно**.
4. На левой панели выберите раздел **Применимые обновления**. Если вы хотите просматривать только установленные обновления, включите параметр **Показывать установленные обновления**.

Отобразится список доступных обновлений приложений сторонних производителей для выбранного устройства.

Экспорт списка доступных обновлений в файл

Вы можете экспортировать список обновлений для приложений сторонних производителей, включая приложения Microsoft, в файл формата CSV или TXT. Вы можете использовать эти файлы, например, чтобы отправить их вашему начальнику по информационной безопасности или сохранить их в целях статистики.

Чтобы экспортировать список доступных обновлений для приложений сторонних производителей в текстовый файл, установленных на всех управляемых устройствах:

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Обновления ПО**.

   Отобразится список доступных обновлений.

   При экспорте полного списка обновлений приложений, будут экспортированы только те обновления, которые отображаются на текущей странице.

   Если вы хотите экспортировать только определенные обновления, установите флажки рядом с требуемыми обновлениями в списке.

2. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать. Если какая-либо из этих кнопок не отображается, нажмите на кнопку с многоточием и выберите нужный вариант в раскрывающемся списке.

Файл, содержащий список доступных обновлений для приложений сторонних производителей, включая приложения Microsoft, загружается на ваше текущее устройство.

Чтобы экспортировать список доступных обновлений для приложений сторонних производителей в текстовый файл, установленных на выбранном управляемом устройстве:

1. Откройте список доступных обновлений приложений сторонних производителей на выбранном управляемом устройстве.

   Отобразится список доступных обновлений.

   При экспорте полного списка обновлений приложений, будут экспортированы только те обновления, которые отображаются на текущей странице.

   Если вы хотите экспортировать только определенные обновления, установите флажки рядом с требуемыми обновлениями в списке.

   Если вы хотите экспортировать только установленные обновления, установите флажок **Показывать установленные обновления**.

2. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать. Если какая-либо из этих кнопок не отображается, нажмите на кнопку с многоточием и выберите нужный вариант в раскрывающемся списке.

Файл, содержащий список доступных обновлений для приложений сторонних производителей, включая приложения Microsoft, установленные на выбранных управляемых устройствах, загружается на ваше текущее устройство.

Одобрение и отклонение обновлений приложений сторонних производителей.

При настройке задачи *Установка требуемых обновлений и закрытие уязвимостей*, вы можете создать правило, для выполнения которого устанавливаемые обновления должны иметь определенный статус. Например, правило обновления может разрешить установку следующего:

- только одобренных обновлений;
- только одобренных обновлений и неопределенных обновлений;
- всех обновлений, независимо от статусов обновлений.

Вы можете подтверждать обновления, которые необходимо установить, и отклонять обновления, которые не должны быть установлены.

При управлении установкой обновлений использовать статуса *Одобрено* целесообразно для небольшого количества обновлений. Чтобы установить несколько обновлений, используйте правила, которые вы можете настроить в свойствах задачи *Установка требуемых обновлений и закрытие уязвимостей*. Рекомендуется устанавливать статус *Одобрено* только для тех обновлений, которые не соответствуют критериям, указанным в правилах. Если вы одобряете вручную большое количество обновлений, производительность Сервера администрирования снижается, что может привести к перегрузке Сервера администрирования.

Чтобы подтвердить или отменить одно или несколько обновлений:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Управление патчами** → **Обновления ПО**.

   Отобразится список доступных обновлений.

2. Выберите обновления, которые требуется подтвердить или отклонить.

3. Нажмите на кнопку **Одобрить**, чтобы одобрить выбранные обновления, или на кнопку **Отклонить**, чтобы отклонить выбранные обновления. Если какая-либо из этих кнопок не отображается, нажмите на кнопку с многоточием и выберите нужный вариант в раскрывающемся списке.

   Статус обновления по умолчанию – *Не определено*.

Выбранные обновления имеют статусы, которые вы указали.

Также вы можете изменить статус в свойствах требуемого обновления.

Чтобы одобрить или отклонить обновление:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Управление патчами** → **Обновления ПО**.

   Отобразится список доступных обновлений.

2. Выберите обновление, которое требуется одобрить или отклонить.

   Откроется окно свойств обновления.

3. В разделе **Общие** выберите статус обновления в раскрывающемся списке **Статус одобрения обновления**. Вы можете выбрать статус *Одобрено*, *Отклонено* или *Не определено*.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Выбранное обновление имеет статус, который вы указали.

Если вы устанавливаете статус *Отклонено* для обновлений стороннего программного обеспечения, то эти обновления не будут устанавливаться на те устройства, для которых они были запланированы к установке, но еще не были установлены. Обновления останутся на тех устройствах, на которые они уже были установлены. При необходимости вы можете удалить их локально вручную.

Создание задачи Установка требуемых обновлений и закрытие уязвимостей

Задача *Установка требуемых обновлений и закрытие уязвимостей* доступна при наличии лицензии на Системное администрирование.

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для обновления и закрытия уязвимостей в приложениях сторонних производителей, установленных на управляемых устройствах. Эта задача позволяет установить несколько обновлений и закрыть несколько уязвимостей в соответствии с правилами, которые вы укажете в параметрах задачи.

Чтобы установить обновления или исправить уязвимости с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей*, вы можете выполнить одно из следующих действий:

- Запустите мастер установки обновлений или мастер закрытия уязвимостей.
- Создайте задачу *Установка требуемых обновлений и закрытие уязвимостей*.
- Добавьте правило для установки обновления в существующую задачу *Установка требуемых обновлений и закрытие уязвимостей*.

Чтобы создать задачу Установка требуемых обновлений и закрытие уязвимостей:

1. В главном окне приложения перейдите в раздел **Задачи**.

2. Нажмите на кнопку **Добавить**.

   Запустится Мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. В раскрывающемся списке **Приложение** выберите Kaspersky Security Center Linux.

4. В списке **Тип задачи** выберите тип задачи **Установка требуемых обновлений и закрытие уязвимостей**.

   Если задача не отображается, проверьте, есть ли у вашей учетной записи права **Чтение**, **Запись** и **Выполнение** в функциональной области **Управление системой**: **Системное администрирование**. Вы не можете создавать и настраивать задачу *Установка требуемых обновлений и закрытие уязвимостей* без этих прав доступа.

5. В поле **Название задачи** укажите название новой задачи.

   Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

6. Выберите устройства, которым будет назначена задача.

7. Добавьте правила установки обновлений на шаге мастера **Задайте правила установки обновлений**

   Эти правила применяются при установке обновлений на клиентские устройства. Если правила не указаны, задача не выполняется. Дополнительную информацию о работе с правилами см. в разделе Правила установки обновлений.

   Эти правила применяются при установке обновлений на клиентские устройства. Если вы не укажете никаких правил, задача не будет выполняться.

8. Задайте следующие параметры:

   - **Начинать установку в момент перезагрузки или выключения устройства**

     Если флажок установлен, установка обновления выполняется перед перезагрузкой или выключением устройства. В противном случае установка обновлений выполняется по расписанию.

     Установите этот флажок, если установка обновлений может повлиять на производительность устройств.

     По умолчанию параметр выключен.

   - **Устанавливать требуемые общесистемные компоненты**

     Если флажок установлен, перед установкой обновления приложение автоматически устанавливает все общесистемные компоненты (пререквизиты), необходимые для установки этого обновления. Например, такими пререквизитами могут являться обновления операционной системы.

     Если этот параметр выключен, необходимо установить пререквизиты вручную.

     По умолчанию параметр выключен.

   - **Разрешать установку новой версии приложения при обновлении**

     Если этот параметр включен, обновления можно устанавливать, только если это приведет к установке новой версии приложения.

     Если этот параметр выключен, приложение не обновляется. Можно позднее установить новые версии приложений вручную или с помощью другой задачи. Например, можно использовать этот параметр, если инфраструктура вашей компании не поддерживает новую версию приложения или если требуется проверить обновление в тестовой инфраструктуре.

     По умолчанию параметр включен.

     > После установки новой версии приложения может быть нарушена работа других приложений, установленных на клиентских устройствах и зависящих от работы обновляемой приложения.

   - **Скачивать обновления на устройство, не устанавливая их**

     Если флажок установлен, приложение загружает обновления на устройство, но не устанавливает их автоматически. Затем вы можете вручную установить загруженные обновления.

     Обновления Microsoft загружаются в служебную папку Windows. Обновления сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) загружаются в папку, указанную в поле **Скачать обновления для**.

     Если этот параметр выключен, обновления автоматически устанавливаются на устройство.

По умолчанию параметр выключен.

- **Скачать обновления для**

  Эта папка используется для загрузки обновлений сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft).

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать файлы трассировки, даже если запись файлов трассировки выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center Linux. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center Linux. Дополнительная трассировка не записывается.

  При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

  По умолчанию параметр выключен.

  - **Максимальный размер файлов расширенной диагностики, МБ**

    По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

Перейдите к следующему шагу мастера.

9. Укажите параметры перезагрузки операционной системы:

- **Не перезагружать устройство**

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

  Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

  По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

  Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

  После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Время ожидания перед принудительным закрытием приложения в заблокированных сеансах через (мин)**

  Принудительное завершение работы приложений, когда устройство пользователя заблокировано (автоматически после периода неактивности или вручную).

  Если параметр включен, работа приложений на заблокированном устройстве принудительно прекращается по истечении времени, указанного в поле ввода.

  Если параметр выключен, работа приложений на заблокированном устройстве не прекращается.

  По умолчанию параметр выключен.

10. Если на шаге мастера **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.

11. Нажмите на кнопку **Готово**.

    В результате работы Мастер создания задачи. 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.

12. 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 выполнения задачи требуемые обновления установлены и уязвимости закрыты.

Если в сети вашей организации используется WSUS-сервер (локальный WSUS-сервер) и вы хотите использовать его вместе с Сервером администрирования, вам нужно сначала убедиться, что Сервер администрирования не используется в качестве WSUS-сервера, и затем выполните следующие действия:

a. На управляемых устройствах с операционной системой Windows указать локальный WSUS-сервер для службы Центра обновления Windows. Вы можете сделать это вручную в реестре Windows или с помощью групповой политики Windows.

b. На локальном WSUS-сервере указать требуемые классификации для обновлений и приложений, по которым они будут распространяться.

c. Синхронизируйте свой WSUS-сервер с вышестоящим сервером (это может быть либо Microsoft WSUS-сервер, либо другой локальный вышестоящий WSUS-сервер).

После запуска задачи *Установка требуемых обновлений и закрытие уязвимостей* на устройстве Агент администрирования использует службу Центра обновления Windows для установки обновлений Windows. Служба Центра обновления Windows получает адрес внешнего WSUS-сервера из реестра и выполняет загрузку обновлений непосредственно с этого внешнего сервера.

Добавление правил для установки обновлений

Эта функциональность доступна при наличии лицензии на Системное администрирование.

При установке обновлений программного обеспечения или закрытии уязвимостей в приложениях с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей* необходимо указать правила установки обновлений. Эти правила определяют обновления для установки и уязвимости к закрытию.

Точные параметры зависят от того, добавляете ли вы правило для всех обновлений Центра обновления Windows или для обновлений приложений сторонних производителей (то есть приложений производства не "Лаборатории Касперского" и не Microsoft). При добавлении правила для обновления Центра обновления Windows или обновления приложений сторонних производителей вы можете выбрать приложения и версии приложений, для которых вы хотите установить обновления. При добавлении правила для всех обновлений вы можете выбрать обновления, которые необходимо установить, и уязвимости, которые вы хотите закрыть с помощью установки обновлений.

Вы можете добавить правило для установки обновлений следующими способами:

- Добавить правило при создании задачи *Установка требуемых обновлений и закрытие уязвимостей*.
- Добавить правило на вкладке **Параметры приложения** в окне свойств существующей задачи *Установка требуемых обновлений и закрытие уязвимостей*.
- С помощью мастера установки обновлений или мастера закрытия уязвимостей.

Добавление правил для всех обновлений

Чтобы добавить правило для всех обновлений:

1. Нажмите на кнопку **Добавить**.

   Будет запущен Мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. На шаге мастера **Выбор типа правила** выберите **Правило для всех обновлений**.

3. На шаге мастера **Общие критерии** укажите следующие параметры:

   - **Набор обновлений для установки**

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.

     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.

     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

     Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

     По умолчанию параметр выключен.

   Перейдите к следующему шагу мастера.

4. Выбор обновлений для установки:

   - **Устанавливать все подходящие обновления**

     В этом случае будут установлены все обновления программного обеспечения, соответствующие критериям, указанным на шаге мастера **Общие критерии**. Выбрано по умолчанию.

   - **Устанавливать только обновления из списка**

     В этом случае будут установлены обновления только того программного обеспечения, которые вы выбираете вручную в списке. Этот список содержит все доступные обновления программного обеспечения.

Например, вы можете задать обновления в следующих случаях: чтобы проверить установку обновлений в тестовом окружении, чтобы обновить только критически важные приложения или чтобы обновить только требуемые приложения.

- **Автоматически устанавливать все предыдущие обновления приложений, необходимые для установки выбранных обновлений**

  Включите этот параметр, если вы согласны с установкой промежуточных версий приложений, когда это необходимо, для установки выбранных обновлений.

  Если этот параметр выключен, устанавливаются только выбранные версии приложений. Выключите этот параметр, если вы хотите непосредственно обновить приложения, не пытаясь последовательно установить версии приложений. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

  Например, у вас на устройстве установлена версия 3 приложения, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

  По умолчанию параметр включен.

Перейдите к следующему шагу мастера.

5. Выберите уязвимости, которые будут закрыты с установкой указанного обновления:

   - **Закрывать все уязвимости, соответствующие остальным критериям**

     В этом случае будут закрыты все уязвимости в приложениях, соответствующие критериям, указанным на шаге мастера **Общие критерии**. Выбрано по умолчанию.

   - **Закрыть только уязвимости из списка**

     Закрывать только уязвимости, которые выбраны вручную в списке. Этот список содержит все обнаруженные уязвимости.

     Например, вы можете задать уязвимости в следующих случаях: чтобы проверить закрытие уязвимостей в тестовом окружении, чтобы закрыть уязвимости только в критически важных приложениях или чтобы закрыть уязвимости только в требуемых приложениях.

   Перейдите к следующему шагу мастера.

6. Укажите название правила, которое вы добавляете. Вы можете изменить имя правила позже, на вкладке **Параметры приложения**, в окне свойств созданной задачи.

Правило будет создано, настроено и отобразится в таблице правил Мастер создания задачи.

Добавление правил для обновлений Центра обновления Windows

Чтобы добавить правило для обновлений Центра обновления Windows:

1. Нажмите на кнопку **Добавить**.

   Будет запущен Мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. Выберите **Правило для обновлений Windows Update**.

   Перейдите к следующему шагу мастера.

3. На шаге мастера **Общие критерии** укажите следующие параметры:

   - **Набор обновлений для установки**

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.

     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.

     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

     Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

     По умолчанию параметр выключен.

   - **Закрывать уязвимости с уровнем критичности по MSRC, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный Microsoft Security Response Center (MSRC), равен или превышает значение, выбранное в списке (**Низкий**, **Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

     Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

     По умолчанию параметр выключен.

4. В окне **Приложения** выберите приложения и версии приложений, для которых вы хотите установить обновления. По умолчанию выбраны все приложения.

5. В окне **Категории обновлений** выберите категории обновлений для установки. Эти категории такие же, как и в каталоге Центра обновления Microsoft. По умолчанию выбраны все категории.

6. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

Добавление правил обновления приложений сторонних производителей

Чтобы добавить правило для обновления приложений сторонних производителей:

1. Нажмите на кнопку **Добавить**.

   Будет запущен Мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. На шаге мастера **Выбор типа правила** выберите **Правило для сторонних обновлений**.

3. На шаге мастера **Общие критерии** укажите следующие параметры:

   - **Набор обновлений для установки**

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.

     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.

     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

     Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

     По умолчанию параметр выключен.

   Перейдите к следующему шагу мастера.

4. Выберите приложения и версии приложений, для которых вы хотите установить обновления.

   По умолчанию выбраны все приложения.

   Перейдите к следующему шагу мастера.

5. Укажите название правила, которое вы добавляете. Вы можете изменить имя правила позже, на вкладке **Параметры приложения**, в окне свойств созданной задачи.

Правило будет создано, настроено и отобразится в таблице правил Мастер создания задачи.

Параметры задачи Установка требуемых обновлений и закрытие уязвимостей, указанные после создания задачи

После создания задачи *Установка требуемых обновлений и закрытие уязвимостей* на вкладке **Параметры приложения** окна свойств задачи вы можете указать следующие параметры:

- В разделе **Проверочная установка**:

  - **Не проверять**. Выберите этот вариант, если вы не хотите выполнять проверочную установку обновлений.

  - **Выполнить проверку на указанных устройствах**. Выберите этот вариант, если вы хотите проверить установку обновлений на определенных устройствах. Нажмите на кнопку **Добавить** и выберите устройства, на которых нужно выполнить проверочную установку обновлений.

  - **Выполнить проверку на устройствах в указанной группе**. Выберите этот вариант, если вы хотите проверить установку обновлений на группе устройств. В поле **Задайте тестовую группу** укажите группу устройств, на которых нужно выполнить проверочную установку.

  - **Выполнить проверку на указанном проценте устройств**. Выберите этот вариант, если вы хотите проверить установку обновлений на определенном количестве устройств. В поле **Процент тестовых устройств из общего числа устройств** укажите процент устройств, на которых нужно выполнить проверочную установку обновлений.

  После выбора любого параметра, кроме **Не проверять**, в поле **Среднее время для принятия решения о продолжении установки (ч)** укажите количество часов, которое должно пройти от тестовой установки обновлений, до начала установки обновлений на все устройства.

- В разделе **Обновления для установки** вы можете просмотреть список обновлений, которые заданы в задаче. Отображаются только обновления, соответствующие параметрам выбранной задачи.

Подробное описание задачи см. в общих параметрах задачи.

Автоматическое обновление приложений сторонних производителей

Некоторые приложения сторонних производителей могут обновляться автоматически. Поставщик приложения определяет, поддерживает ли приложение функцию автоматического обновления. Если приложение стороннего производителя, установленное на управляемом устройстве, поддерживает автоматическое обновление, вы можете указать параметр автоматического обновления в свойствах приложения. После изменения параметра автоматического обновления Агенты администрирования применяют новый параметр на каждом управляемом устройстве, на котором установлено приложение.

Параметр автоматического обновления не зависит от других объектов и возможностей Системного администрирования. Например, этот параметр не зависит от статуса одобрения обновления или задач установки обновления, таких как *Установка требуемых обновлений и закрытие уязвимостей* и *Закрытие уязвимостей*.

Чтобы настроить параметр автоматического обновления для приложения стороннего производителя:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Реестр приложений**.

2. Нажмите на имя приложения, для которого вы хотите изменить параметр автоматического обновления.

   Чтобы упростить поиск, вы можете отфильтровать список по столбцам **Статус автоматических обновлений** и **Управление автоматическим обновлением**.

   Откроется окно свойств приложения.

3. В разделе **Общие** выберите значение для следующей функции:

   Статус автоматических обновлений

   Выберите один из следующих вариантов:

   - **Не определено**

     Функция автоматического обновления выключена. Kaspersky Security Center Linux устанавливает обновления приложений сторонних производителей с помощью задач: *Установка требуемых обновлений и закрытие уязвимостей* и *Закрытие уязвимостей*.

   - **Разрешено**

     После того как поставщик выпускает обновление для приложения, это обновление автоматически устанавливается на управляемые устройства. Никаких дополнительных действий не требуется.

   - **Заблокировано**

     Обновления приложения не устанавливаются автоматически. Kaspersky Security Center Linux устанавливает обновления приложений сторонних производителей с помощью задач: *Установка требуемых обновлений и закрытие уязвимостей* и *Закрытие уязвимостей*.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Настройка автоматического обновления применяется к выбранному приложению.

Закрытие уязвимостей в приложениях сторонних производителей

В этом разделе описаны возможности Kaspersky Security Center Linux связанные с закрытием уязвимостей в приложениях, установленных на управляемых устройствах.

Об обнаружении и закрытии уязвимостей в приложениях

Kaspersky Security Center Linux обнаруживает и закрывает уязвимости в приложениях на управляемых устройствах под управлением операционных систем Microsoft Windows. Уязвимости обнаруживаются в операционной системе и в стороннем программном обеспечении, включая программное обеспечение Microsoft.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

Обнаружение уязвимостей в приложениях

Для обнаружения уязвимостей Kaspersky Security Center Linux выполняет поиск известных уязвимостей в приложениях на основе признаков из баз данных об известных уязвимостях. База данных создана и поддерживается специалистами "Лаборатории Касперского" в актуальном состоянии. Она содержит информацию об уязвимостях, такую как описание уязвимостей, дата обнаружения уязвимостей и уровень критичности уязвимостей. Информация об уязвимостях в приложениях приведена на сайте "Лаборатории Касперского".

В Kaspersky Security Center Linux для поиска уязвимостей в приложениях используется задача *Поиск уязвимостей и требуемых обновлений*.

Закрытие уязвимостей в приложениях

Для закрытия уязвимостей в приложениях, Kaspersky Security Center Linux использует обновления программного обеспечения выпущенные поставщиками программного обеспечения. Метаданные обновлений программного обеспечения загружаются в хранилище Сервера администрирования в результате выполнения задачи *Загрузка обновлений в хранилище Сервера администрирования*. Эта задача предназначена для загрузки метаданных обновлений для приложений "Лаборатории Касперского" и приложений сторонних производителей. Эта задача автоматически создается в мастере первоначальной настройки Kaspersky Security Center Linux. Вы также можете вручную создать задачу *Загрузка обновлений в хранилище Сервера администрирования*.

Обновления программного обеспечения для закрытия уязвимостей могут быть представлены в виде полных дистрибутивов или патчей. Обновления программного обеспечения, которые закрывают уязвимости в приложениях, называются *исправлениями*. *Рекомендуемые исправления* это исправления, которые рекомендуются к установке специалистами "Лаборатории Касперского". *Пользовательские исправления* это исправления, которые вручную указываются для установки пользователями. Чтобы установить пользовательское исправление, необходимо создать инсталляционный пакет, содержащий это исправление.

Если лицензия Kaspersky Security Center Linux предусматривает возможности Системного администрирования, используйте задачу *Установка требуемых обновлений и закрытие уязвимостей*. Эта задача автоматически закрывает несколько уязвимостей, устанавливая рекомендуемые исправления. Для этой задачи вы можете вручную настроить определенные правила для закрытия нескольких уязвимостей.

Если лицензия Kaspersky Security Center Linux не предусматривает возможности Системного администрирования, используйте задачу *Закрытие уязвимостей*. С помощью этой задачи можно закрыть уязвимости, установив рекомендуемые исправления для приложений Microsoft и пользовательских исправлений для приложений сторонних производителей.

Из соображений безопасности любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных приложений с помощью технологий "Лаборатории Касперского". Эти технологии используются для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение.

Эксперты "Лаборатории Касперского" не проводят ручной анализ обновлений приложений сторонних производителей, которые можно установить с помощью Системного администрирования. Также эксперты "Лаборатории Касперского" не занимаются поиском уязвимостей (известных или неизвестных) или недокументированных возможностей в таких обновлениях и не проводят другие виды анализа упомянутых выше обновлений.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Для закрытия некоторых уязвимостей программного обеспечения вам нужно принять Лицензионное соглашение для установки программного обеспечения, если это требуется. Если вы отклоняете Лицензионное соглашение, уязвимость в программном обеспечении не закроется.

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей

В этом разделе представлен сценарий обнаружения и закрытия уязвимостей на управляемых устройствах под управлением Windows. Вы можете обнаружить и закрыть уязвимости в операционной системе и в стороннем программном обеспечении, включая программное обеспечение Microsoft.

Предварительные требования

- Kaspersky Security Center Linux развернут в вашей организации.
- В сети вашей организации есть управляемые устройства под управлением Windows.
- Подключение Сервера администрирования к интернету необходимо для выполнения следующих задач:
  - Составление списка рекомендуемых исправлений уязвимостей в приложениях Microsoft. Список формируется и регулярно обновляется специалистами "Лаборатории Касперского".
  - Закрытие уязвимостей в приложениях сторонних производителей, отличных от приложений Microsoft.

Этапы

Обнаружение и закрытие уязвимостей состоит из следующих этапов:

1. **Поиск уязвимостей в программном обеспечении, установленном на управляемых устройствах**

   Чтобы найти уязвимости в приложениях, установленных на управляемых устройствах, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Kaspersky Security Center Linux получает список обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, указанных в свойствах задачи и установленных на устройствах.

   Задача *Поиск уязвимостей и требуемых обновлений* автоматически создается в мастере первоначальной настройки Kaspersky Security Center Linux. Если вы не запускали мастер первоначальной настройки, запустите его сейчас или создайте задачу вручную.

   > Вы можете создать задачу *Поиск уязвимостей и требуемых обновлений* только для устройств под управлением Windows. Вы не можете создать эту задачу для устройств, работающих под управлением других операционных систем.

2. **Просмотр списка обнаруженных уязвимостей в приложениях**

   Просмотрите список **Уязвимости в приложениях** и решите, какие уязвимости нужно закрыть. Чтобы просмотреть подробную информацию о каждой уязвимости, нажмите на имя уязвимости в списке. Для каждой уязвимости в списке вы также можете просмотреть статистику уязвимости на управляемых устройствах.

3. **Настройка закрытия уязвимостей**

   Обнаружив уязвимости в приложениях, вы можете закрыть их на управляемых устройствах с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей* или задачи *Закрытие уязвимостей*.

   Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для обновления и закрытия уязвимостей в приложениях сторонних производителей, в том числе в приложениях Microsoft, установленных на управляемых устройствах. Эта задача позволяет установить несколько обновлений и закрыть несколько уязвимостей в соответствии с определенными правилами. Обратите внимание, что эту задачу можно создать, только если у вас есть лицензия на Системное администрирование. Чтобы устранить уязвимости в приложениях, задача *Установка требуемых обновлений и закрытие уязвимостей* использует рекомендованные обновления приложений.

   Задача *Закрытие уязвимостей* не требует лицензии для Системного администрирования. Чтобы использовать эту задачу, требуется вручную указать пользовательские исправления для закрытия уязвимостей в приложениях сторонних производителей, которые указаны в параметрах задачи. Задача *Закрытие уязвимостей* использует рекомендованные исправления приложений Microsoft и пользовательские исправления для приложений сторонних производителей.

   > Вы можете создать задачу *Установка требуемых обновлений и закрытие уязвимостей* и задачу *Закрытие уязвимостей* только для устройств под управлением Windows. Вы не можете создать эти задачи для устройств, работающих под управлением других операционных систем.

   Вы можете запустить мастер закрытия уязвимостей, который автоматически создаст одну из этих задач, или вы можете создать одну из этих задач вручную.

Если вы создали и настроили задачу *Установка требуемых обновлений и закрытие уязвимостей*, уязвимости будут автоматически закрыты на управляемых устройствах. При запуске созданной задачи, задача сопоставляет список доступных обновлений программного обеспечения с правилами, указанными в параметрах задачи. Все обновления программного обеспечения, которые соответствуют критериям в указанных правилах, загружены в хранилище Сервера администрирования и установлены для закрытия уязвимостей в приложениях.

Если вы создали задачу *Закрытие уязвимостей*, закрываются только уязвимости в приложениях Microsoft.

4. **Задание расписания задачи**

   Запланируйте автоматическое выполнение задачи *Поиск уязвимостей и требуемых обновлений* на периодической основе, чтобы поддерживать актуальность списка уязвимостей. Рекомендуемый период – один раз в неделю.

   Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете задать ее запуск с той же периодичностью, что и для задачи *Поиск уязвимостей и требуемых обновлений*, или реже. При задании расписания задачи *Закрытие уязвимостей*, вам нужно выбрать исправления приложений Microsoft или указать пользовательские исправления для приложений сторонних производителей каждый раз перед запуском задачи.

   При задании расписания задач убедитесь, что задача закрытия уязвимостей запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

5. **Игнорирование уязвимостей в приложениях (если требуется)**

   Вы можете игнорировать уязвимость в определенных приложениях на всех управляемых устройствах или только на выбранных управляемых устройствах.

6. **Запуск задачи закрытия уязвимости**

   Запустите задачу *Установка требуемых обновлений и закрытие уязвимостей* или *Закрытие уязвимостей*. Когда задача будет завершена, убедитесь, что в списке задач она имеет статус *Завершена успешно*.

7. **Создание отчета о результатах закрытия уязвимостей в приложениях (если требуется)**

   Чтобы просмотреть статистику о закрытых уязвимостях, сформируйте отчет об уязвимостях. В этом отчете отображается информация об уязвимостях в приложениях, которые не закрыты. Он позволяет выявлять и закрывать уязвимости в программном обеспечении сторонних производителей, включая программное обеспечение Microsoft, которое используется в вашей организации.

8. **Проверка настройки обнаружения и закрытия уязвимостей в приложениях сторонних производителей**

   Убедитесь, что вы выполнили следующее:

   - обнаружили и просмотрели список уязвимостей в приложениях на управляемых устройствах;
   - проигнорировали некоторые уязвимости в приложениях, по желанию;
   - настроили задачу закрытия уязвимости;
   - запланировали запуск задач для поиска и закрытия уязвимостей в приложениях так, чтобы они запускались последовательно;
   - проверили, что задача закрытия уязвимостей была запущена.

Закрытие уязвимостей в приложениях сторонних производителей

Чтобы найти уязвимости в приложениях сторонних производителей, вы можете создать и запустить задачу *Поиск уязвимостей и требуемых обновлений* и получить список уязвимостей в приложениях. После получения списка уязвимостей в приложениях вы можете закрыть уязвимости на управляемых устройствах с операционными системами Windows.

Вы можете закрыть уязвимости в операционной системе и приложениях сторонних производителей, включая программное обеспечение Microsoft, создав и запустив задачу *Закрытие уязвимостей* или задачу *Установка требуемых обновлений и закрытие уязвимостей*.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Также вы можете создать задачу для закрытия уязвимостей в приложениях следующими способами:

- Откройте список уязвимостей и укажите, какие уязвимости необходимо закрыть.

  В результате создается задача закрытия уязвимостей в приложениях. Также можно добавить выбранные уязвимости в существующую задачу.

- Запустите мастер закрытия уязвимостей.

  Мастер закрытия уязвимости доступен при наличии лицензии на Системное администрирование.

  Мастер упрощает создание и настройку задачи закрытия уязвимостей, а также исключает создание избыточных задач.

Закрытие уязвимостей в приложениях с помощью списка уязвимостей

Чтобы закрыть уязвимости в приложениях с помощью списка уязвимостей:

1. Откройте список уязвимостей для изменения, выполнив одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Управление патчами** → **Уязвимости в приложениях**.
   - В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства** → имя устройства → **Дополнительно** → **Уязвимости в приложениях**.
   - В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Сторонние приложения** → **Реестр приложений** → <название приложения> → **Уязвимости**.

   Откроется страница со списком уязвимостей в приложениях сторонних производителей, установленных на управляемых устройствах.

2. В списке уязвимостей установите флажки рядом с уязвимостями, которые вы хотите закрыть и нажмите на кнопку **Закрыть уязвимость**.

   Если рекомендуемое обновление программного обеспечения для закрытия одной из выбранных уязвимостей отсутствует, отображается информационное сообщение.

Для закрытия некоторых уязвимостей в приложениях вам нужно принять Лицензионное соглашение для установки приложений, если это требуется. Если вы отклоняете Лицензионное соглашение, уязвимость в приложении не закроется.

3. Выберите один из следующих вариантов:

   - **Новая задача**

     Запустится Мастер создания задачи. Если у вас есть лицензия на Системное администрирование, по умолчанию выбирается тип задачи *Установка требуемых обновлений и закрытие уязвимостей*. Если у вас нет лицензии, по умолчанию выбирается тип задачи *Закрытие уязвимостей*. Следуйте далее указаниям мастера, чтобы завершить создание задачи.

   - **Закрыть уязвимость (добавить правило в указанную задачу)**

     Выберите задачу, в которую вы хотите добавить выбранные уязвимости. Если у вас есть лицензия на Системное администрирование, выберите задачу *Установка требуемых обновлений и закрытие уязвимостей*. В выбранную задачу будет автоматически добавлено новое правило для закрытия выбранных уязвимостей. Если у вас нет лицензии, по умолчанию выбран тип задачи *Закрытие уязвимостей*. Выбранные уязвимости добавлены в свойства задачи.

     Откроется окно свойств задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы выбрали создание задачи, она создается и отображается в списке задач в разделе **Задачи**. Если вы выбрали добавление уязвимостей в существующую задачу, уязвимости сохраняются в свойствах задачи.

Чтобы закрыть уязвимости в приложениях сторонних производителей, запустите задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Закрытие уязвимостей*. Если вы создали задачу *Закрытие уязвимостей*, вам нужно вручную указать обновления программного обеспечения, перечисленных в свойствах задачи.

Закрытие уязвимостей в приложениях с помощью мастера закрытия уязвимостей

Мастер закрытия уязвимости доступен при наличии лицензии на Системное администрирование.

Чтобы закрыть уязвимости в приложениях с помощью мастера закрытия уязвимостей:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Управление патчами** → **Уязвимости в приложениях**.

   Откроется таблица со списком уязвимостей в приложениях сторонних производителей, установленных на управляемых устройствах.

2. Установите флажок напротив уязвимости, которую требуется закрыть.

3. Нажмите на кнопку **Запустить мастер закрытия уязвимости**.

   Кнопка недоступна, если вы выбрали более одной уязвимости.

Откроется мастер закрытия уязвимости. Отобразится список существующих задач. В списке могут присутствовать следующие типы задач:

- *Установка требуемых обновлений и закрытие уязвимостей*
- *Закрытие уязвимостей*

Вы не можете изменить задачу *Закрытие уязвимостей* чтобы установить новые обновлений. Для установки новых обновлений можно использовать только задачу *Установка требуемых обновлений и закрытие уязвимостей*.

4. Если вы хотите, чтобы мастер отображал только те задачи, которые закрывают выбранную уязвимость, включите параметр **Показывать только задачи, которые закрывают выбранную уязвимость**.

5. Выполните одно из следующих действий:

   - Чтобы запустить задачу, установите флажок рядом с именем задачи и нажмите на кнопку **Запустить**.

     Никаких дальнейших действий не требуется. Вы можете закрыть мастер. Задача выполняется в фоновом режиме.

   - Чтобы добавить правило в существующую задачу *Установка требуемых обновлений и закрытие уязвимостей*.

     a. Установите флажок рядом с именем задачи и нажмите на кнопку **Добавить правило**.

     > Кнопка **Добавить правило** недоступна, если вы выбрали более одной задачи.

     Вы не можете добавить правило для задачи *Закрытие уязвимостей*. Если вы выбрали задачу *Закрытие уязвимостей*, появится следующее уведомление: "Для установки обновлений используйте задачу "Установка требуемых обновлений и закрытие уязвимостей"".

     b. На открывшейся странице настройте новое правило:

     - **Правило закрытия уязвимостей данного уровня критичности**

       Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

       Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение важности выбранного обновления (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

       Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

       По умолчанию параметр выключен.

     - **Правило для закрытия уязвимостей с помощью обновлений того же типа, что и обновление, определенное в соответствии с рекомендациями для выбранной уязвимости**

       Это правило отображается только для уязвимостей в приложениях Microsoft.

     - **Правило закрытия уязвимостей в приложениях выбранного поставщика**

       Это правило отображается только для уязвимостей сторонних приложений.

- **Правило закрытия уязвимости во всех версиях выбранного приложения**

  Это правило отображается только для уязвимостей сторонних приложений.

- **Правило закрытия выбранной уязвимости**

- **Одобрить обновления, закрывающие выбранную уязвимость**

  Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

  По умолчанию параметр выключен.

c. Нажмите на кнопку **Добавить**.

Откроется окно свойств задачи. Новое правило уже добавлено в свойства задачи. Вы можете просмотреть или изменить правило, а также другие параметры задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

- Чтобы создать задачу:

a. Нажмите на кнопку **Новая задача**.

b. На открывшейся странице настройте новое правило:

- **Правило закрытия уязвимостей данного уровня критичности**

  Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

  Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение важности выбранного обновления (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

  Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

  По умолчанию параметр выключен.

- **Правило для закрытия уязвимостей с помощью обновлений того же типа, что и обновление, определенное в соответствии с рекомендациями для выбранной уязвимости**

  Это правило отображается только для уязвимостей в приложениях Microsoft.

- **Правило закрытия уязвимостей в приложениях выбранного поставщика**

  Это правило отображается только для уязвимостей сторонних приложений.

- **Правило закрытия уязвимости во всех версиях выбранного приложения**

  Это правило отображается только для уязвимостей сторонних приложений.

- **Правило закрытия выбранной уязвимости**

- **Одобрить обновления, закрывающие выбранную уязвимость**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

c. Нажмите на кнопку **Добавить**.

d. Продолжите создавать задачу в Мастер создания задачи.

Новое правило, добавленное в мастер закрытия уязвимости, отображается на шаге мастера **Задайте правила установки обновлений**. После завершения работы мастера задача *Установка требуемых обновлений и закрытие уязвимостей* добавлена в список задач.

Создание задачи Закрытие уязвимостей

Задача *Закрытие уязвимостей* позволяет закрыть уязвимости в приложениях на управляемых устройствах. Вы можете закрыть уязвимости в приложениях сторонних производителей, включая приложения Microsoft.

Вы можете создать задачу *Закрытие уязвимостей* только для устройств под управлением Windows. Вы не можете создать эту задачу для устройств, работающих под управлением других операционных систем.

Вы можете создать задачи *Закрытие уязвимостей*, только если у вас есть лицензия на Системное администрирование.

Чтобы закрыть новые уязвимости, вы можете добавить их в существующую задачу *Закрытие уязвимостей*. Рекомендуется использовать задачу *Установка требуемых обновлений и закрытие уязвимостей* вместо задачи *Закрытие уязвимостей*. Задача *Установка требуемых обновлений и закрытие уязвимостей* позволяет автоматически устанавливать несколько обновлений и закрывать несколько уязвимостей в соответствии с заданными правилами.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Чтобы создать задачу Закрытие уязвимостей:

1. В главном окне приложения перейдите в раздел **Задачи**.

   Вы также можете создать эту задачу в окне свойств устройства на вкладке **Задачи**.

2. Нажмите на кнопку **Добавить**.

   Запустится Мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. В раскрывающемся списке **Приложение** выберите Kaspersky Security Center.

4. В списке **Тип задачи** выберите тип задачи **Закрытие уязвимостей**.

5. В поле **Название задачи** укажите название новой задачи.

   Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

6. Выберите устройства, которым будет назначена задача.

   Перейдите к следующему шагу мастера.

7. Нажмите на кнопку **Добавить**.

   Откроется список уязвимостей.

8. В списке уязвимостей установите флажки рядом с уязвимостями, которые вы хотите закрыть, и нажмите на кнопку **OK**.

   Для уязвимостей в приложениях Microsoft обычно существуют рекомендуемые исправления. Дополнительные действия для них не требуются.

   Для уязвимостей в приложениях сторонних производителей сначала необходимо указать исправление пользователя для каждой уязвимости, которую вы хотите закрыть. После этого вы сможете добавить эти уязвимости в задачу *Закрытие уязвимостей*.

   Перейдите к следующему шагу мастера.

9. Укажите параметры перезагрузки операционной системы:

   - **Не перезагружать устройство**

     Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

   - **Перезагрузить устройство**

     В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

   - **Запрашивать у пользователя**

     На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

     По умолчанию выбран этот вариант.

   - **Повторять запрос каждые (мин)**

     Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

     По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

     Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

  После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать приложения в заблокированных сеансах**

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.

Перейдите к следующему шагу мастера.

10. Задайте параметры учетной записи:

    - **Учетная запись по умолчанию**

      Задача будет запускаться под той же учетной записью, под которой было установлено и запущено приложение, выполняющее эту задачу.

      По умолчанию выбран этот вариант.

    - **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.

11. Если на шаге мастера **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 в разделе **Задачи**.

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 выполнения задачи выбранные уязвимости закрыты.

Пользовательские исправления для уязвимостей в приложениях сторонних производителей

Чтобы использовать задачу *Закрытие уязвимостей*, необходимо вручную указать обновления программного обеспечения, чтобы закрыть уязвимости в приложениях сторонних производителей, перечисленные в параметрах задачи. Задача *Закрытие уязвимостей* использует рекомендованные исправления приложений Microsoft и пользовательские исправления для других приложений сторонних производителей.

Пользовательские исправления – это обновления программного обеспечения, которые администратор вручную указывает для установки, чтобы закрыть уязвимости.

Чтобы выбрать пользовательские исправления для уязвимостей в приложениях сторонних производителей:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Управление патчами** → **Уязвимости в приложениях**.

   Откроется страница со списком уязвимостей в приложениях сторонних производителей, установленных на управляемых устройствах.

2. В списке уязвимостей в приложениях перейдите по ссылке с названием уязвимости, для которой вы хотите указать пользовательское исправление.

   Откроется окно свойств выбранной уязвимости.

3. На левой панели выберите раздел **Пользовательские и другие исправления**.

   Отобразится список пользовательских исправлений для выбранной уязвимости в приложениях.

4. Нажмите на кнопку **Добавить**.

   Отобразится список доступных инсталляционных пакетов. Список отобразившихся инсталляционных пакетов соответствует списку в папке **Управление программным обеспечением** → **Инсталляционные пакеты**.

   Если вы не создали инсталляционный пакет, содержащий пользовательское исправление для закрытия выбранной уязвимости, вы можете создать пакет сейчас, нажав на кнопку **Новый** и запустив мастер создания инсталляционного пакета.

5. Выберите инсталляционный пакет (или пакеты), содержащий пользовательское исправление (или пользовательские исправления) для выбранной уязвимости.

6. Нажмите на кнопку **Сохранить**.

Указаны инсталляционные пакеты, содержащие пользовательские исправления для уязвимости в приложениях. Когда вы запускаете задачу *Закрытие уязвимостей*, инсталляционный пакет устанавливается и уязвимость в приложении закрывается.

Просмотр информации об уязвимостях в приложениях, обнаруженных на всех управляемых устройствах

После проверки программного обеспечения на управляемых устройствах на наличие уязвимостей вы можете просмотреть список обнаруженных уязвимостей в приложениях. Если вы запустите задачу для иерархии Серверов администрирования, вы можете просмотреть список управляемых устройств с обнаруженными уязвимостями только для выбранного Сервера администрирования.

Вы также можете сформировать и просмотреть отчет об уязвимостях.

Чтобы просмотреть список уязвимостей в приложениях, обнаруженных на всех управляемых устройствах,

В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

Отобразится список уязвимостей в приложениях, обнаруженных на клиентских устройствах.

Чтобы настроить список уязвимостей в приложениях,

Нажмите на значок **Фильтр** ( ) в верхнем правом углу списка уязвимостей в приложениях и выберите нужный фильтр. Вы также можете выбрать один из предустановленных фильтров в раскрывающемся списке **Предустановленные фильтры** над списком уязвимостей в приложениях.

Вы можете получить подробную информацию о любой уязвимости из списка.

Чтобы получить информацию об уязвимости в приложениях,

в списке уязвимостей в приложениях перейдите по ссылке с названием уязвимости.

Откроется окно свойств уязвимости в приложениях.

Просмотр информации об уязвимостях в приложениях, обнаруженных на выбранных управляемых устройствах

Вы можете просмотреть информацию об уязвимостях в приложениях, обнаруженных на выбранном управляемом устройстве под управлением Windows.

Чтобы просмотреть список уязвимостей в приложениях, обнаруженных на выбранном управляемом устройстве:

1. В главном окне приложения перейдите в раздел **Управление активами → Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием устройства, для которого вы хотите просмотреть обнаруженные уязвимости в приложениях.

   Откроется окно свойств выбранного устройства.

3. В окне свойств выбранного устройства выберите вкладку **Дополнительно**.

4. На левой панели выберите раздел **Уязвимости в приложениях**.

Отобразится список уязвимостей в приложениях, обнаруженных на выбранном управляемом устройстве.

Чтобы просмотреть свойства выбранной уязвимости в приложениях,

перейдите по ссылке с названием уязвимости в списке уязвимостей в приложениях.

Откроется окно свойств выбранной уязвимости в приложениях.

Просмотр статистики уязвимостей на управляемых устройствах.

Вы можете просмотреть статистическую информацию каждой уязвимости в приложениях на управляемых устройствах. Статистика представлена в виде диаграмм. На диаграмме отображается количество устройств со следующими статусами:

- *Игнорируется на: <количество устройств>*. Этот статус присваивается, если в свойствах уязвимости вы вручную установили параметр игнорировать уязвимость.
- *Закрыта на: <количество устройств>*. Этот статус присваивается, если задача закрытия уязвимости успешно завершена.
- *Запланирована к закрытию на: <количество устройств>*. Этот статус присваивается, если вы создали задачу закрытия уязвимостей, но задача пока еще не завершена.
- *Применено исправление на: <количество устройств>*. Этот статус присваивается, если вы вручную выбрали обновление программного обеспечения, чтобы закрыть уязвимость, но это обновление не закрыло уязвимость.
- *Требует закрытия на: <количество устройств>*. Этот статус присваивается, если уязвимость была закрыта только на некоторых управляемых устройствах, а уязвимость требуется закрыть на других управляемых устройствах.

Чтобы просмотреть статистику уязвимости на управляемых устройствах:

1. В главном окне приложения перейдите в раздел **Операции → Управление патчами → Уязвимости в приложениях**.

   Отобразится страница со списком уязвимостей в приложениях, обнаруженных на управляемых устройствах.

2. Установите флажок рядом с требуемой уязвимостью.

3. Нажмите на кнопку **Статистика уязвимостей на устройствах**.

   Кнопка **Статистика уязвимостей на устройствах** недоступна, если вы выбрали более одной уязвимости.

Отобразится диаграмма статусов уязвимости. Нажав на статус, откроется список устройств, на которых уязвимость имеет выбранный статус.

Экспорт списка уязвимостей в приложениях в текстовый файл

Вы можете скачать список отображаемых уязвимостей в файл формата CSV или TXT. Вы можете отправить эти файлы специалисту по безопасности или сохранить их для статистических целей.

Чтобы экспортировать список уязвимостей в приложениях, обнаруженных на всех управляемых устройствах, в текстовый файл:

1. В главном окне приложения перейдите в раздел **Операции → Управление патчами → Уязвимости в приложениях**.

   Отображается список уязвимостей в приложениях, обнаруженных на управляемых устройствах.

   По умолчанию экспортируются только уязвимости, отображаемые на текущей странице.

   Если вы хотите экспортировать только определенные уязвимости, установите флажки рядом с этими уязвимостями.

2. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать. Если какая-либо из этих кнопок не отображается, нажмите на кнопку с многоточием и выберите нужный вариант в раскрывающемся списке.

На ваше устройство загружается файл со списком уязвимостей в приложениях.

Чтобы просмотреть список уязвимостей в приложениях, обнаруженных на выбранном управляемом устройстве:

1. В главном окне приложения перейдите в раздел **Управление активами → Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием устройства, для которого вы хотите просмотреть обнаруженные уязвимости в приложениях.

   Откроется окно свойств выбранного устройства.

3. В окне свойств выбранного устройства выберите вкладку **Дополнительно**.

4. На левой панели выберите раздел **Уязвимости в приложениях**.

Отобразится список уязвимостей в приложениях, обнаруженных на выбранном управляемом устройстве.

По умолчанию экспортируются только уязвимости, отображаемые на текущей странице.

Если вы хотите экспортировать только определенные уязвимости, установите флажки рядом с этими уязвимостями.

1. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать. Если какая-либо из этих кнопок не отображается, нажмите на кнопку с многоточием и выберите нужный вариант в раскрывающемся списке.

На ваше устройство загружается файл со списком уязвимостей в приложениях.

Игнорирование уязвимостей в приложениях

Вы можете игнорировать уязвимости в приложениях и не закрывать их. Причины для игнорирования уязвимостей в приложениях могут быть, например, следующими:

- Вы не считаете, что уязвимость в приложении является критической для вашей организации.
- Вы понимаете, что закрытие уязвимости в приложениях может повредить данные приложения, для которого требуется закрыть уязвимость.
- Вы уверены, что уязвимость в приложениях не представляет опасности для сети вашей организации, так как вы используете другие меры для защиты управляемых устройств.

Вы можете игнорировать уязвимость в приложениях на всех управляемых устройствах или только на выбранных управляемых устройствах.

Чтобы пропустить уязвимость в приложениях на всех управляемых устройствах:

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

   Отображается список уязвимостей в приложениях, обнаруженных на управляемых устройствах.

2. В списке уязвимостей в приложениях нажмите на имя уязвимости в приложениях, которую вы хотите пропустить.

   Откроется окно свойств уязвимости в приложениях.

3. На вкладке **Общие** включите параметр **Игнорировать уязвимость**.

4. Нажмите на кнопку **Сохранить**.

   Окно свойств уязвимости в приложениях закроется.

Уязвимость в приложениях пропускается на всех управляемых устройствах.

Чтобы пропустить уязвимость в приложениях на выбранных управляемых устройствах:

1. В главном окне приложения перейдите в раздел **Управление активами → Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с именем устройства, на котором вы хотите пропустить уязвимость в приложениях.

   Откроется окно свойств устройства.

3. В окне свойств устройства выберите раздел **Дополнительно**.

4. На левой панели выберите раздел **Уязвимости в приложениях**.

   Отобразится список уязвимостей в приложениях, обнаруженных на устройстве.

5. В списке уязвимостей в приложениях выберите уязвимость, которую вы хотите пропустить на выбранном устройстве.

   Откроется окно свойств уязвимости в приложениях.

6. В окне свойств уязвимости в приложениях на вкладке **Общие** включите параметр **Игнорировать уязвимость**.

7. Нажмите на кнопку **Сохранить**.

   Окно свойств уязвимости в приложениях закроется.

8. Закройте окно свойств устройства.

Уязвимость в приложениях пропускается на выбранном устройстве.

Пропущенные уязвимости в приложениях не будут закрыты после завершения работы задачи *Закрытие уязвимостей* и задачи *Установка требуемых обновлений и закрытие уязвимостей*. Вы можете исключить пропущенные уязвимости в приложениях из списка уязвимостей с помощью фильтра.

Создание инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"

Kaspersky Security Center Web Console позволяет выполнять удаленную установку приложений сторонних производителей с помощью инсталляционных пакетов. Такие приложения сторонних производителей включены в соответствующую базу данных "Лаборатории Касперского". База данных создается автоматически при первом запуске задачи *Загрузка обновлений в хранилище Сервера администрирования*.

Вы можете создать инсталляционный пакет приложения стороннего производителя из базы данных "Лаборатории Касперского" только если у вас есть лицензия на Системное администрирование.

Чтобы создать инсталляционный пакет для приложения стороннего производителя из базы "Лаборатории Касперского":

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Инсталляционные пакеты**.

2. Нажмите на кнопку **Добавить**.

   Запустится Мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Выберите параметр **Выбрать приложение из базы "Лаборатории Касперского" для создания инсталляционного пакета**.

   > Этот параметр доступен при наличии лицензии на Системное администрирование.

   Перейдите к следующему шагу мастера.

4. Выберите приложение, для которого требуется создать инсталляционный пакет.

   Перейдите к следующему шагу мастера.

5. Выберите нужный язык локализации в раскрывающемся списке и нажмите на кнопку Далее.

   > Этот шаг отображается только если приложение предоставляет несколько языков.

6. Если вам будет предложено принять Лицензионное соглашение для установки, на шаге мастера **Лицензионные соглашения и Политики конфиденциальности** выполните следующие действия:

   a. Перейдите по ссылке **Показать**, чтобы прочитать Лицензионное соглашение на веб-сайте поставщика или просмотреть обновления, для которых требуется лицензия.

   b. Установите флажок **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения настоящего Лицензионного соглашения**.

   c. Нажмите на кнопку **Принять все**, чтобы принять все Лицензионные соглашения и Политики конфиденциальности, отображаемые в списке.

7. На шаге мастера **Имя нового инсталляционного пакета** в поле **Имя пакета** укажите имя инсталляционного пакета и нажмите на кнопку **Далее**.

   Созданный инсталляционный пакет загружен на Сервер администрирования. Мастер создания инсталляционного пакета отображает сообщение об успешном создании инсталляционного пакета.

8. Нажмите на кнопку **Готово**.

Созданный инсталляционный пакет отображается в списке инсталляционных пакетов. Вы можете выбрать этот пакет при создании или перенастройке задачи *Удаленная установка приложения*.

> Вы можете создать и перенастроить задачу *Удаленная установка приложения* с помощью инсталляционного пакета приложения стороннего производителя из базы данных "Лаборатории Касперского", только если у вас есть лицензия на Системное администрирование.

Просмотр и изменение параметров инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"

Если вы ранее создавали какие-либо инсталляционные пакеты приложений сторонних производителей, перечисленные в базе "Лаборатории Касперского", вы можете просмотреть и изменить параметры этих пакетов.

Изменение параметров инсталляционного пакета приложения стороннего производителя из базы "Лаборатории Касперского" доступно только при наличии лицензии на Системное администрирование.

Чтобы просмотреть и изменить параметры инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского":

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Инсталляционные пакеты**.
2. В открывшемся списке инсталляционных пакетов нажмите на имя соответствующего пакета.

   Откроется окно свойств.
3. При необходимости измените параметры.
4. Нажмите на кнопку **Сохранить**.

   Изменения сохранены.

Параметры инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"

Параметры инсталляционного пакета приложения стороннего производителя сгруппированы на следующих вкладках:

Не все параметры, перечисленные ниже, отображаются по умолчанию. Вы можете добавить нужные столбцы, нажав на кнопку **Фильтр** и выбрав соответствующие имена столбцов из списка.

- Вкладка **Общие**:
  - Поле ввода, содержащее название инсталляционного пакета, которое можно изменить вручную.
  - **Приложение**

    Имя приложения стороннего производителя, для которого создан инсталляционный пакет.

- **Версия**

  Номер версии приложения стороннего производителя, для которого создан инсталляционный пакет.

- **Размер**

  Размер инсталляционного пакета для приложения стороннего производителя (в килобайтах).

- **Создан**

  Дата и время создания инсталляционного пакета для приложения стороннего производителя.

- **Путь**

  Полный путь к сетевой папке, в которой находится инсталляционный пакет для приложения стороннего производителя.

- Вкладка **Последовательность установки**:

  - **Устанавливать требуемые общесистемные компоненты**

    Если флажок установлен, перед установкой обновления приложение автоматически устанавливает все общесистемные компоненты (пререквизиты), необходимые для установки этого обновления. Например, такими пререквизитами могут являться обновления операционной системы.

    Если этот параметр выключен, необходимо установить пререквизиты вручную.

    По умолчанию параметр выключен.

  - Таблица, в которой отображаются свойства обновления и которая содержит следующие графы:

    - **Имя**

      Название обновления.

    - **Описание**

      Описание обновления.

    - **Источник**

      Источник обновления, то есть выпущено ли обновление Microsoft или другим сторонним производителем.

    - **Тип**

      Тип обновления, то есть предназначено ли обновление для драйвера или приложения.

    - **Категория**

      Категория служб Windows Server Update Services (WSUS), отображаемая для обновлений Microsoft (Критические обновления, Обновления определений, Драйверы, Пакеты дополнительных компонентов, Обновления системы безопасности, Пакеты обновления, Средства, Накопительные пакеты обновления, Обновления или Обновления с предыдущих версий).

    - **Уровень важности по MSRC**

      Уровень важности обновления, определенный Microsoft Security Response Center (MSRC).

- **Уровень важности**

  Уровень важности обновления определен "Лабораторией Касперского".

- **Уровень важности патча**

  Уровень важности патча, если он предназначен для приложений "Лаборатории Касперского".

- **Статья**

  Идентификатор статьи в Базе знаний с описанием обновления.

- **Бюллетень**

  Идентификатор бюллетеня безопасности с описанием обновления.

- **Не назначено к установке (новая версия)**

  Отображается, имеет ли обновление статус Не назначено к установке.

- **Назначено к установке**

  Отображается, имеет ли обновление статус Назначено к установке.

- **Устанавливается**

  Отображается, имеет ли обновление статус Устанавливается.

- **Установлено**

  Отображается, имеет ли обновление состояние Установлено.

- **Сбой**

  Отображается, имеет ли обновление статус Сбой.

- **Требуется перезагрузка**

  Отображается, имеет ли обновление статус Требуется перезагрузка.

- **Зарегистрировано**

  Отображается дата и время, когда обновление было зарегистрировано.

- **Устанавливается интерактивно**

  Отображается, требуется ли взаимодействие с пользователем во время установки обновления.

- **Статус одобрения обновления**

  Отображается, одобрена ли установка обновления.

- **Ревизия**

  Отображается номер текущей ревизии обновления.

- **Идентификатор обновления**

  Отображается идентификатор обновления.

- **Версия приложения**

  Отображается номер версии, до которой должно быть обновлено приложение.

- **Заменяемое**

  Отображаются другие обновления, которые могут заменить это обновление.

- **Заменяющее**

  Отображаются другие обновления, которые можно заменить этим обновлением.

- **Требуется принять условия Лицензионного соглашения**

  Отображается, требует ли обновление согласие с условиями Лицензионного соглашения.

- **Описание веб-адреса**

  Отображается имя поставщика обновлений.

- **Семейство приложений**

  Отображается имя семейства приложений, к которым относится обновление.

- **Приложение**

  Отображается название приложения, которому принадлежит обновление.

- **Язык локализации**

  Отображается язык локализации обновления.

- **Не назначено к установке (новая версия)**

  Отображается, имеет ли обновление статус Не назначено к установке (новая версия).

- **Требует установки пререквизитов**

  Отображается, имеет ли обновление состояние Требует установки пререквизитов.

- **Режим загрузки**

  Отображается режим загрузки обновлений.

- **Является патчем**

  Отображается, является ли обновление патчем.

- **Не установлено**

  Отображается, имеет ли обновление статус Не установлено.

- **Создан**

- Вкладка **Параметры**, на которой отображаются параметры инсталляционного пакета, их названия, описания и значения, которые используются в качестве параметров командной строки во время установки. Если в пакете таких нет параметров, отображается соответствующее сообщение. Вы можете изменить значения этих параметров.

- Вкладка **История ревизий**, на которой отображается версии инсталляционного пакета и которая содержит следующие графы:
  - **Ревизия** – номер версии инсталляционного пакета.
  - **Время** – дата и время изменения параметров инсталляционного пакета.
  - **Пользователь** – имя пользователя, изменившего параметры инсталляционного пакета.
  - **IP-адрес устройства пользователя** – IP-адрес устройства, с которого был изменен объект.
  - **IP-адрес Web Console** – IP-адрес приложения Kaspersky Security Center Web Console, с помощью которого был изменен объект.
  - **Действие** – действия, которые были выполнены с инсталляционным пакетом в этой ревизии.
  - **Описание** – описание ревизии изменения параметров инсталляционного пакета.

    По умолчанию описание ревизии не заполнено. Чтобы добавить описание ревизии, выберите нужную ревизию и нажмите на кнопку **Изменить описание**. В открывшемся окне введите текст описания ревизии.

Закрытие уязвимостей в изолированной сети

В этом разделе описаны действия, которые вы можете предпринять для закрытия уязвимостей в приложениях сторонних производителей на управляемых устройствах, подключенных к Серверам администрирования и не имеющих доступа в интернет.

Сценарий: закрытие уязвимостей в приложениях сторонних производителей в изолированной сети

Вы можете устанавливать обновления и закрывать уязвимости приложений сторонних производителей, установленных на управляемых устройствах в изолированной сети. К таким сетям относятся Серверы администрирования и подключенные к ним управляемые устройства, не имеющие доступа в интернет. Для закрытия уязвимостей в такой сети необходим Сервер администрирования, подключенный к интернету. Используя Сервер администрирования с доступом в интернет, вы сможете загружать патчи (необходимые обновления) и передавать их на изолированные Серверы администрирования.

> Вы можете загружать обновления приложений сторонних производителей, выпущенные производителями программного обеспечения, но не можете загружать обновления для программного обеспечения Microsoft на изолированных Серверах администрирования с помощью Kaspersky Security Center.

Подробнее о процессе закрытия уязвимостей в изолированной сети, ознакомьтесь с описанием и схемой этого процесса.

Предварительные требования

Перед началом сделайте следующее:

1. Выделите одно устройство для подключения к интернету и загрузки исправлений. Это устройство будет считаться Сервером администрирования с доступом в интернет.
2. Установите Kaspersky Security Center Linux версии не ниже 15.1 на следующих устройствах:
   - Выделенное устройство, которое будет выступать в роли Сервера администрирования с доступом в интернет.
   - Изолированные устройства, которые будут выступать в роли изолированных от интернета Серверов администрирования (далее – изолированные Серверы администрирования).
3. Убедитесь, что на каждом Сервере администрирования достаточно места на диске для загрузки и хранения обновлений и исправлений.

Этапы

Установка обновлений и закрытие уязвимостей в приложениях сторонних производителей на управляемых устройствах, относящихся к изолированным Серверам администрирования, состоит из следующих этапов:

1. **Настройка Сервера администрирования с доступом в интернет**

   Подготовьте Сервер администрирования с доступом в интернет для обработки запросов на необходимые обновления стороннего программного обеспечения и для загрузки.

2. **Настройка изолированных Серверов администрирования**

   Подготовьте изолированные Серверы администрирования, чтобы они могли регулярно формировать списки необходимых обновлений и обрабатывать патчи, загружаемые Сервером администрирования с доступом в интернет. После настройки изолированные Серверы администрирования больше не пытаются загружать патчи из интернета. Вместо этого они получают обновления через патчи.

3. **Передача патчей и установка обновлений на изолированные Серверы администрирования**

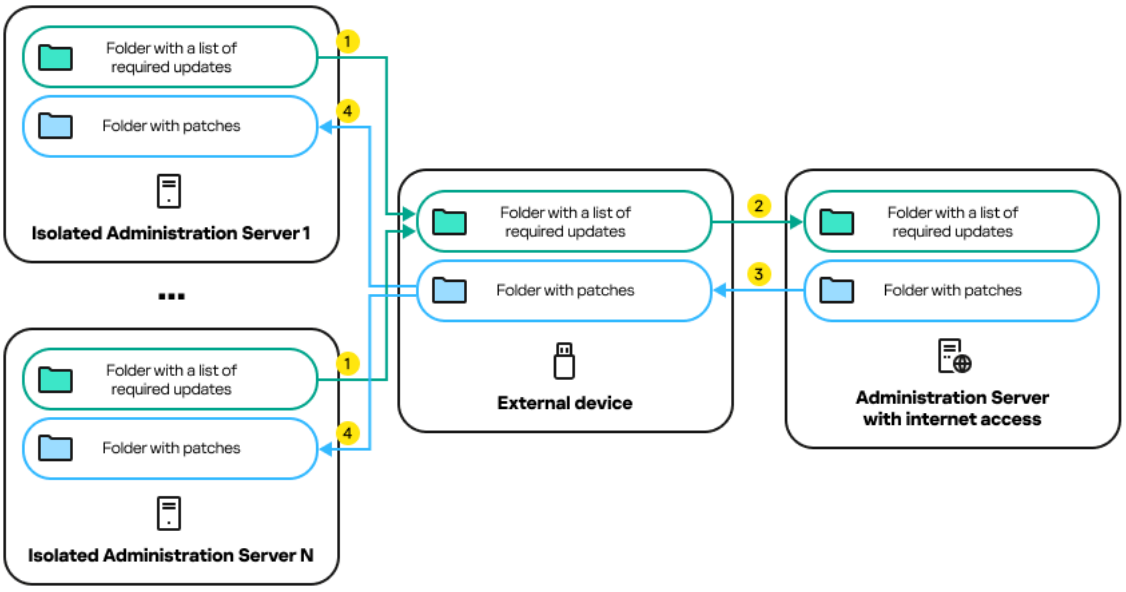
   Когда настройка Серверов администрирования закончена, вы можете переносить списки обновлений и патчи с Сервера администрирования, имеющего доступ интернет, на изолированные Серверы администрирования. Далее обновления из исправлений будут установлены на управляемые устройства с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей*.

Результаты

Таким образом обновления приложений сторонних производителей передаются на изолированные Серверы администрирования и устанавливаются на подключенные управляемые устройства с помощью Kaspersky Security Center Linux. Достаточно один раз настроить Серверы администрирования, чтобы получать обновления с нужной вам частотой, например, один или несколько раз в день.

О закрытии уязвимостей в приложениях сторонних производителей в изолированной сети

Процесс закрытия уязвимостей в приложениях сторонних производителей в изолированной сети показан на рисунке ниже. Вы можете периодически повторять этот процесс.



Процесс передачи патчей и списка необходимых обновлений между Сервером администрирования с доступом в интернет и изолированными Серверами администрирования

Каждый Сервер администрирования, изолированный от сети интернет (далее – изолированный Сервер администрирования), формирует список обновлений, которые нужно установить на управляемые устройства, подключенные к этому Серверу администрирования. Этот список обновлений хранится в определенной папке в виде набора двоичных файлов, каждый из которых имеет идентификатор патча, содержащего необходимое обновление. Поэтому каждый файл в списке соответствует определенному патчу.

Список требуемых обновлений переносится с изолированного Сервера администрирования на выделенный Сервер администрирования с доступом в интернет с помощью внешнего устройства. После этого назначенный Сервер администрирования загружает патчи из интернета и помещает их в назначенную папку.

Когда все патчи загружены и помещены в указанную папку, они переносятся обратно на каждый изолированный Сервер администрирования, с которого был получен список необходимых обновлений. Патчи сохраняются в специально созданной для них папке на каждом изолированном Сервере администрирования.

В результате задача *Установка требуемых обновлений и закрытие уязвимостей* запускает патчи и устанавливает обновления на управляемые устройства изолированных Серверов администрирования.

Настройка Сервера администрирования с доступом в интернет для закрытия уязвимостей в изолированной сети

Чтобы подготовиться к закрытию уязвимостей и передаче патчей в изолированной сети, сначала настройте Сервер администрирования с доступом в интернет, а затем настройте изолированные Серверы администрирования.

Чтобы настроить Сервер администрирования с доступом в интернет:

1. Создайте две папки на диске, где установлен Сервер администрирования:

   - папку для списка необходимых обновлений;
   - папку для патчей.

   Вы можете назвать эти папки по своему желанию.

2. Предоставьте группе KLAdmins право **Изменение** на созданные папки, используя стандартные средства администрирования операционной системы.

3. С помощью утилиты klscflag укажите пути к папкам в свойствах Сервера администрирования.

   Запустите командную строку и измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag находится в директории, в которой установлен Сервер администрирования. По умолчанию задан путь /opt/kaspersky/ksc64/sbin.

4. Выполните следующие команды в командной строке:

   - Чтобы указать путь к папке для исправлений:
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<path to the folder>"`
   - Чтобы задать путь к папке для списка необходимых обновлений:
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<path to the folder>"`

   Пример: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "/Folder_for_patches"`

5. При необходимости с помощью утилиты klscflag укажите, как часто Сервер администрирования должен проверять наличие новых запросов на исправления:
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <value in seconds>`

   По умолчанию указано значение 120 секунд.

   Пример: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 120`

6. Создайте задачу *Поиск уязвимостей и требуемых обновлений*, чтобы получить информацию о патчах для приложений сторонних производителей, установленных на управляемых устройствах, и настройте расписание выполнения задачи.

7. Создайте задачу *Закрытие уязвимостей*, чтобы указать патчи для приложений сторонних производителей, используемых для закрытия уязвимостей, и настройте расписание задачи.

   Запустите задачи вручную, если вы хотите, чтобы они выполнялись раньше, чем указано в расписании задачи. Порядок запуска задач важен. Задачу *Закрытие уязвимостей* необходимо запустить после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

8. Перезапустите службу Сервера администрирования.

Сервер администрирования с доступом в интернет готов к загрузке и передаче обновлений на изолированные Серверы администрирования. Прежде чем приступить к закрытию уязвимостей, настройте изолированные Серверы администрирования.

Настройка изолированных Серверов администрирования для закрытия уязвимостей в изолированной сети

После настройки Сервера администрирования с доступом в интернет, подготовьте каждый изолированный Сервер администрирования в вашей сети, чтобы закрывать уязвимости и устанавливать обновления на управляемых устройствах, подключенных к этим изолированным Серверам администрирования.

Чтобы настроить изолированные Серверы администрирования, выполните следующие действия для каждого Сервера администрирования:

1. Активируйте лицензионный ключ для Системного администрирования.
2. Создайте две папки на диске, где установлен Сервер администрирования:
   - папку для списка необходимых обновлений;
   - папку для патчей.

   Вы можете назвать эти папки по своему желанию.
3. Предоставьте группе KLAdmins право **Изменение** на созданные папки, используя стандартные средства администрирования операционной системы.
4. С помощью утилиты klscflag укажите пути к папкам в свойствах Сервера администрирования.

   Запустите командную строку и измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag находится в директории, в которой установлен Сервер администрирования. По умолчанию задан путь /opt/kaspersky/ksc64/sbin.
5. Выполните следующие команды в командной строке:
   - Чтобы указать путь к папке для исправлений:
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<путь к папке>"`
   - Чтобы задать путь к папке для списка необходимых обновлений:
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<путь к папке>"`

   Пример: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "/FolderForPatches"`
6. При необходимости с помощью утилиты klscflag укажите, как часто изолированный Сервер администрирования должен проверять наличие новых патчей:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <значение в секундах>`

   По умолчанию указано значение 120 секунд.

   Пример: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 120`
7. При необходимости с используйте утилиту klscflag для вычисления хешей SHA256 патчей:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1`

   Выполнив эту команду, вы можете убедиться, что патчи не были изменены при их переносе на изолированный Сервер администрирования и что вы получили корректные патчи, содержащие необходимые обновления.

По умолчанию Kaspersky Security Center Linux не вычисляет хеши SHA256 патчей. Если включить этот параметр, после получения патчей изолированным Сервером администрирования Kaspersky Security Center Linux вычисляет их хеши и сравнивает полученные значения с хешами, хранящимися в базе данных Сервера администрирования. Если вычисленный хеш не совпадает с хешем в базе данных, возникает ошибка и вам необходимо заменить неверные патчи.

8. Создайте задачу *Поиск уязвимостей и требуемых обновлений*, чтобы получить информацию о патчах для приложений сторонних производителей, установленных на управляемых устройствах, и настройте расписание выполнения задачи.

9. Создайте задачу *Закрытие уязвимостей*, чтобы указать патчи для приложений сторонних производителей, используемых для закрытия уязвимостей, и настройте расписание задачи.

   Запустите задачи вручную, если вы хотите, чтобы они выполнялись раньше, чем указано в расписании задачи. Порядок запуска задач важен. Задачу *Закрытие уязвимостей* необходимо запустить после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

10. Перезапустите службу Сервера администрирования.

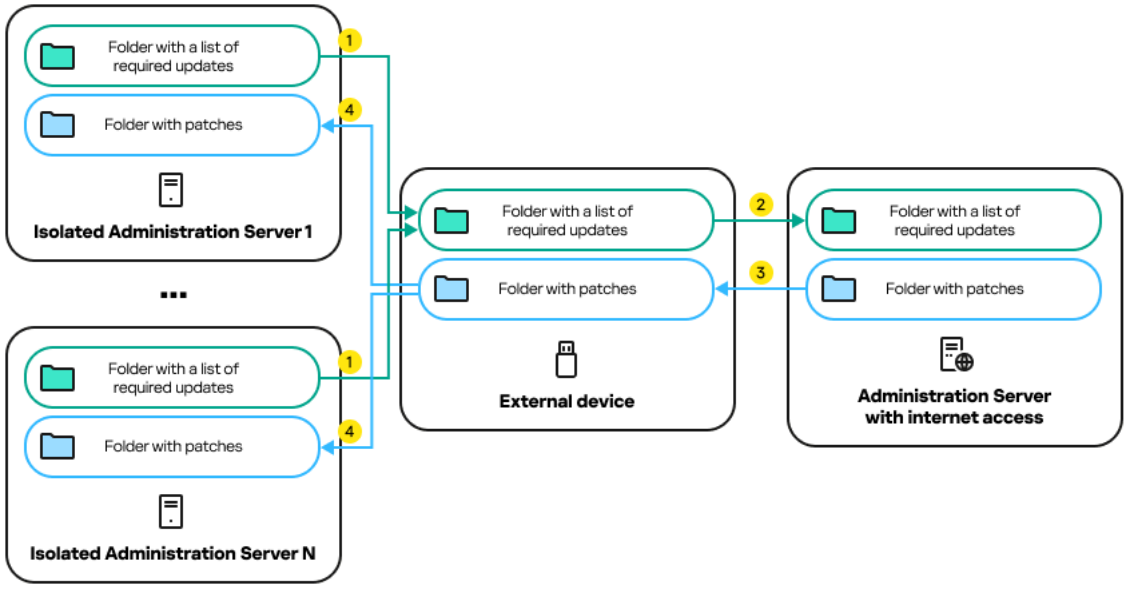
После настройки всех Серверов администрирования вы можете переместить исправления и списки необходимых обновлений и закрыть уязвимости приложений сторонних производителей на управляемых устройствах в изолированной сети.

Передача исправлений и установка обновлений в изолированной сети

После того, как настройка Серверов администрирования закончена, вы можете переносить патчи с необходимыми обновлениями с Сервера администрирования, имеющего доступ интернет, на изолированные Серверы администрирования. Вы можете передавать и устанавливать обновления с нужной вам частотой, например, один или несколько раз в день.

Съемный диск, например, внешний диск, необходим, для переноса патчей и списка необходимых обновлений между Серверами администрирования. Убедитесь, что внешний диск имеет достаточно места для загрузки и хранения патчей.

Процесс передачи патчей и списка необходимых обновлений показан на рисунке ниже:



Процесс передачи патчей и списка необходимых обновлений между Сервером администрирования с доступом в интернет и изолированными Серверами администрирования

Чтобы установить обновления и закрыть уязвимости на управляемых устройствах, подключенных к изолированным Серверам администрирования:

1. Запустите задачу *Установка требуемых обновлений и закрытие уязвимостей*, если она еще не запущена.

2. Подключите внешний диск к любому изолированному Серверу администрирования.

3. Создайте на внешнем диске две папки: одну для списка необходимых обновлений и одну для патчей. Вы можете назвать эти папки по своему желанию.

   Если вы создали эти папки ранее, очистите их.

4. Скопируйте список необходимых обновлений с каждого изолированного Сервера администрирования и вставьте этот список в папку для списка необходимых обновлений на внешнем диске.

   В результате вы объединяете все списки, полученные со всех изолированных Серверов администрирования, в одну папку. В этой папке должны находиться бинарные файлы с идентификаторами патчей, необходимых для всех изолированных Серверов администрирования.

5. Подключите внешний диск к Серверу администрирования с доступом в интернет.

6. Скопируйте список необходимых обновлений с внешнего диска и вставьте этот список в папку для списка необходимых обновлений на Сервере администрирования с доступом в интернет.

   Все необходимые патчи автоматически загружаются из интернета в папку патчей на Сервере администрирования. Это может занять несколько часов.

7. Убедитесь, что все необходимые патчей загружены. Для этого можно выполнить одно из следующих действий:

   - Проверьте папку на наличие патчей на Сервере администрирования с доступом в интернет. Все исправления, которые были указаны в списке необходимых обновлений, должны быть загружены в нужную папку. Это удобнее, если требуется небольшое количество исправлений.

   - Подготовьте специальный скрипт, например, shell-скрипт. Если вы получите большое количество патчи, то будет сложно самостоятельно проверить, что все исправления загружены. В таких случаях лучше автоматизировать проверку.

8. Скопируйте патчи с Сервера администрирования с доступом в интернет и вставьте их в соответствующую папку на внешнем диске.

9. Перенесите исправления на каждый изолированный Сервер администрирования. Поместите патчи в специальную папку для них.

   В результате каждый изолированный Сервер администрирования формирует актуальный список обновлений, необходимых для управляемых устройств, подключенных к текущему Серверу администрирования. После получения списка необходимых обновлений Сервер администрирования загружает из интернета патчи. При появлении этих патчей на изолированных Серверах администрирования задача *Установка требуемых обновлений и закрытие уязвимостей* обрабатывает патчи. Таким образом, на управляемые устройства устанавливаются обновления и закрываются уязвимости в приложениях сторонних производителей.

При выполнении задачи *Установка требуемых обновлений и закрытие уязвимостей* не перезагружайте устройство Сервера администрирования и не запускайте задачу *Резервное копирование данных Сервера администрирования* (это также вызовет перезагрузку). В результате задача *Установка требуемых обновлений и закрытие уязвимостей* прерывается, а обновления не устанавливаются. В этом случае вам необходимо перезапустить эту задачу вручную или дождаться запуска задачи по настроенному расписанию.

Выключение передачи патчей и установка обновлений в изолированной сети

Вы можете выключить передачу исправлений на изолированные Сервера администрирования, например, если вы решили вывести один или несколько Серверов администрирования из изолированной сети. Таким образом вы сможете уменьшить количество исправлений и время на их загрузку.

Чтобы выключить передачу исправлений на изолированные Серверы администрирования:

1. Если вы хотите вывести из изоляции все Серверы администрирования, в свойствах Сервера администрирования с доступом в интернет удалите пути к предполагаемым папкам для патчей и список необходимых обновлений. Если вы хотите, чтобы выбранные Серверы администрирования находились в изолированной сети, пропустите этот шаг.

   Запустите командную строку и измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag находится в директории, в которой установлен Сервер администрирования. По умолчанию задан путь /opt/kaspersky/ksc64/sbin.

   Выполните следующие команды в командной строке:

   - Чтобы удалить путь к папке с патчами:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```

- Чтобы удалить путь к папке со списком необходимых обновлений:
  ```
  klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
  ```

2. Перезапустите службу Сервера администрирования с доступом в интернет, если вы удалили пути к папкам.

3. В свойствах каждого изолированного Сервера администрирования, который вы хотите вывести из изоляции, удалите пути к папкам для патчей и список необходимых обновлений.

   Выполните следующие команды в командной строке под учетной записью с правами root:

   - Чтобы удалить путь к папке с патчами:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
     ```

   - Чтобы удалить путь к папке со списком необходимых обновлений:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
     ```

4. Перезапустите службу каждого Сервера администрирования, на котором вы удалили пути к папкам.

Если вы перенастроили Сервер администрирования с выходом в интернет, патчи больше не будут передаваться через Kaspersky Security Center Linux.

Если вы перенастроили только определенные Серверы администрирования и удалили их из изолированной сети, они больше не будут получать патчи через Kaspersky Security Center Linux. Только те Серверы администрирования, которые остаются в изолированной сети, будут продолжать получать исправления.

Если вы хотите в будущем приступить к закрытию уязвимостей на отключенных изолированных Серверах администрирования, вам необходимо настроить эти Серверы администрирования и Сервер администрирования с доступом в интернет еще раз.

Справочное руководство API

Справочное руководство по Kaspersky Security Center OpenAPI предназначено для решения следующих задач:

- Автоматизация и настройка. Вы можете автоматизировать задачи, которые, возможно, не хотите выполнять вручную. Например, как администратор вы можете использовать Kaspersky Security Center OpenAPI для создания и запуска сценариев, которые упростят разработку структуры групп администрирования и поддержат ее в актуальном состоянии.

- Пользовательская разработка. Используя OpenAPI, вы можете разработать клиентское приложение.

Вы можете использовать поле поиска в правой части экрана, чтобы найти нужную информацию в справочном руководстве OpenAPI.

Справочное руководство OpenAPI

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 Linux или назначать точки распространения. Вы можете запускать примеры как есть или создавать собственные сценарии на их основе.

Чтобы вызвать методы OpenAPI и запустить скрипт,

Установите пакет KlAkOAPI из архива KlAkOAPI.tar.gz на устройстве, на котором установлен Сервер администрирования.

Пакет KlAkOAPI включает в себя набор примеров типовых операций. Вызывать методы OpenAPI, запускать примеры и свои сценарии можно только на устройствах, на которых установлены Сервер администрирования и пакет KlAkOAPI. Архив KlAkOAPI.tar.gz, содержащий этот пакет, находится в папке установки Kaspersky Security Center Linux.

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

Пример	Назначение примера	Сценарий
Загрузите файлы списка сетей с помощью шлюза соединения на указанное устройство	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
Установка лицензионного ключа, хранящегося в хранилище главного Сервера администрирования, на подчиненные Серверы администрирования	Вы можете подключиться к главному Серверу администрирования, загрузить с него необходимый лицензионный ключ и передать этот ключ на все подчиненные Серверы администрирования, входящие в иерархию.	Лицензирование управляемых приложений
Создание отчета об эффективных правах пользователей	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
Запуск задачи на устройстве	Вы можете подключиться к Агенту администрирования на нужном устройстве, используя шлюз соединения, а затем запустить необходимую задачу.	Запуск задачи вручную
Регистрация точек распространения для устройств в группе	Вы можете назначить управляемые устройства точками распространения (ранее они назывались "агенты обновлений").	Обновление баз и приложений "Лаборатории Касперского"
Перечисление всех групп	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
Перечисление задач, запрос статистики задач и запуск задач	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
Создание и запуск задачи	Вы можете создать задачу. Укажите в примере следующие параметры задачи: • Тип. • Способ запуска. • Название. • Группа устройств, для которой будет использоваться задача. По умолчанию в примере создается задача типа "Показать сообщение". Вы можете запустить эту задачу для всех управляемых устройств Сервера администрирования. При необходимости вы можете указать свои параметры задачи.	Создание задачи
Перечисление лицензионных ключей	Вы можете получить список всех активных лицензионных ключей для приложений "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
Создание и поиск внутреннего пользователя	Вы можете создать учетную запись для дальнейшей работы.	Добавление учетной записи внутреннего пользователя
Создание пользовательской категории	Вы можете создать категорию приложений с требуемыми параметрами.	Создание пополняемой вручную категории приложений

Пример	Назначение примера	Сценарий
Перечисление пользователей с помощью SrvView	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
Создание внутренних пользователей, создание инсталляционного пакета Android и отправка его по электронной почте	Вы можете создать внутренних пользователей с помощью класса SecurityPolicy, создать инсталляционный пакет Android и отправить его пользователям по электронной почте.	Добавление учетной записи внутреннего пользователя

Приложения, взаимодействующие с Kaspersky Security Center Linux через OpenAPI

Некоторые приложения взаимодействуют с Kaspersky Security Center Linux через OpenAPI. К таким приложениям относятся, например, Kaspersky Anti Targeted Attack Platform или Kaspersky Security для виртуальных сред. Это также может быть пользовательское клиентское приложение, разработанное вами на основе OpenAPI.

Приложения, взаимодействующие с Kaspersky Security Center Linux 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 приложения, использующие Kaspersky Security Center Linux OpenAPI. Чтобы узнать, работает ли используемое вами приложение с OpenAPI, обратитесь к справке этого приложения.

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 приложения, а также способы решения типичных проблем, возникающих при работе приложения.

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 Web Console;

- 8060 TCP – порт HTTP для публикации автономных пакетов средствами Kaspersky Security Center Web Console;
- 13292 TCP – данный TLS-порт нужен, только если требуется управлять мобильными устройствами;
- 8080 TCP – порт HTTPS для Kaspersky Security Center 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. Вам 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 соединения. 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

Устройства с установленным Агентом администрирования могут быть использованы в качестве точки распространения. В этом режиме Агент администрирования может выполнять следующие функции:

- Передачу файлов на клиентские устройства, включая:
  - Базы и модули приложений "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 приложений 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;
  - опрашивать 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 этой 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

Некоторые компании-клиенты, например MSP-клиенты, могут использовать несколько Серверов администрирования. Администрировать несколько разрозненных Серверов неудобно, поэтому целесообразно объединять их в иерархию. Сервер администрирования с операционной системой Linux может работать в иерархии Серверов как в качестве главного Сервера, так и в качестве подчиненного Сервера. Главный Сервер с операционной системой Linux может управлять подчиненными Серверами с операционными системами и Linux и Windows. Главный Сервер с операционной системой Windows может управлять подчиненным Сервером с операционной системой Linux.

Взаимодействие "главный – подчиненный" между двумя Серверами администрирования предоставляет следующие возможности:

- Подчиненный Сервер наследует с главного Сервера политики, задачи, роли пользователей и инсталляционные пакеты, устраняется дублирование параметров.
- Выборки устройств на главном Сервере могут включать в себя устройства с подчиненных Серверов.
- Отчеты на главном Сервере могут включать в себя данные (в том числе и детальные) с подчиненных Серверов.
- Главный Сервер администрирования может использоваться в качестве источника обновлений для подчиненного Сервера администрирования.

Главный Сервер администрирования получает данные только от невиртуальных подчиненных Серверов администрирования в рамках перечисленных выше параметров. Это ограничение не распространяется на виртуальные Серверы администрирования, которые совместно используют базу данных со своим главным Сервером администрирования.

Иерархия Серверов администрирования поддерживает мультитенантный режим. Этот режим позволяет Главному администратору централизованно управлять независимо несколькими клиентами. Каждая организация-клиент или офис изолированы от других и называются тенантами. Вы можете выделить несколько управляемых устройств вместе со связанными с ними данными, параметрами, политиками и задачами для тенанта, а также настроить права пользователей для каждого тенанта.

Главный Сервер администрирования, установленный в основной инфраструктуре организации, выполняет в роль главного тенанта. Главный Сервер администрирования позволяет подчиненным или виртуальным Серверам администрирования (и его изолированным тенантам) независимо получать и обрабатывать свои события, а также работать со своими ресурсами, службами и конфигурациями.

Поставщик услуг, у которого есть несколько организаций-клиентов, может предоставить функциональность Kaspersky Security Center Linux, включая агрегирование алертов и действия по реагированию, каждой организации-клиенту независимо. Для этого поставщик услуг подключает подчиненные или виртуальные Серверы администрирования в качестве тенантов для каждой организации-клиента. Поставщик услуг предоставляет услуги, используя свой собственный персонал и ресурсы.

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 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 приложений 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 распределенным приложением. В состав Kaspersky Security Center Linux входят следующие приложения:

- Сервер администрирования – центральный компонент, ответственный за управление устройствами организации и хранение данных в СУБД.
- Kaspersky Security Center 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 приложением 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 Web Console;
- установка Агента администрирования и приложения 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 Linux на отказоустойчивом кластере, вам нужно создать учетные записи для служб Kaspersky Security Center Linux.

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 запустить один Сервер администрирования менее чем на 20 000 устройствах.
MariaDB (см. поддерживаемые версии)	Используйте эту СУБД, если вы планируете запустить один Сервер администрирования менее чем на 20 000 устройствах.

PostgreSQL, Postgres Pro (см. поддерживаемые версии)	Используйте эту СУБД, если вы планируете запустить один Сервер администрирования менее чем на 50 000 устройствах.
Tantor (см. поддерживаемые версии)	Используйте эту СУБД, если вы планируете запустить один Сервер администрирования менее чем на 50 000 устройствах. СУБД Tantor поддерживается только в Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8).

Подробнее о том как установить выбранную СУБД, см. в документации к этой СУБД.

Рекомендуется выключить задачу инвентаризации программного обеспечения и выключить (в параметрах политики Kaspersky Endpoint Security) уведомления Сервера администрирования о запуске приложений.

Если вы решили установить СУБД PostgreSQL или Postgres Pro, убедитесь, что вы указали пароль для суперпользователя. Если пароль не указан, Сервер администрирования может не подключиться к базе данных.

Если вы установите 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 Web Console, однако при этом он не изменится автоматически в уже созданных инсталляционных пакетах Агента администрирования.

Поддержка неактивных подключений

Для улучшения стабильности соединения рекомендуется настроить следующие параметры keepalive на устройствах шлюза соединения:

- `net.ipv4.tcp_keepalive_intvl` указывает, как часто нужно отправлять сообщения keepalive после первого сообщения. Установите для этого параметра значение `1`.
- `net.ipv4.tcp_keepalive_probes` указывает, сколько сообщений keepalive можно отправить без ответа, прежде чем соединение будет считаться потерянным. Установите для этого параметра значение `10`.
- `net.ipv4.tcp_keepalive_time` указывает, как долго ждать после последнего пакета данных перед отправкой первого сообщения keepalive. Установите для этого параметра значение `900`.

Чтобы настроить параметры keepalive:

1. Откройте файл the /etc/sysctl.conf.
2. Добавьте следующие значения параметров:

```
net.ipv4.tcp_keepalive_intvl = 1
net.ipv4.tcp_keepalive_probes = 10
net.ipv4.tcp_keepalive_time = 900
```

3. Выполните следующую команду, чтобы обновить параметры keepalive:

```
sudo sysctl -p /etc/sysctl.conf
```

4. Выполните следующие команды, чтобы убедиться, что значения параметров были применены:

```
sudo sysctl net.ipv4.tcp_keepalive_intvl
sudo sysctl net.ipv4.tcp_keepalive_probes
sudo sysctl net.ipv4.tcp_keepalive_time
```

Развертывание Агента администрирования и приложений безопасности

Для управления устройствами в организации и для их защиты от угроз безопасности, вам нужно установить Агент администрирования и приложение безопасности "Лаборатории Касперского" на каждое устройство.

Подробнее о развертывании защиты см. раздел Развертывание Агента администрирования и приложения безопасности.

Подробнее о защите мобильных устройств см. раздел Управление мобильными устройствами.

В Microsoft Windows XP Агент администрирования может некорректно выполнять следующие операции: загрузка обновлений напрямую с серверов "Лаборатории Касперского" (если выполняет роль точки распространения); функционирование в качестве прокси-сервера KSN (если выполняет роль точки распространения); обнаружение уязвимостей приложений сторонних производителей (при использовании Системного администрирования).

Настройка защиты в сети организации-клиента

После завершения установки Сервера администрирования запускается приложение Kaspersky Security Center Web Console, которое 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 приложений 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, вам нужно 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 **Настройка**.
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 **Настройка**.
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 приложениях**. Если этот флажок установлен, в базе данных Сервера администрирования сохраняется информация о всех версиях всех модулей приложений на устройствах в сети организации. Указанная информация может занимать значительный объем в базе данных Kaspersky Security Center Linux (десятки гигабайтов). Поэтому, если в политике верхнего уровня по-прежнему установлен флажок **О запускаемых приложениях**, его необходимо снять.

Раздел Дополнительные параметры, подраздел Интерфейс

Если управление защитой от угроз в сети организации необходимо выполнять централизованно через Kaspersky Security Center Web Console, следует выключить отображение пользовательского интерфейса Kaspersky Endpoint Security на рабочих станциях (сняв флажок **Отображать интерфейс приложения** 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 Агент администрирования будет подключаться к той точке распространения, маршрут к которой является самым коротким. Маршрут к точке распространения можно определить с помощью утилиты tracert или утилиты traceroute.

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 приложения P, определенной для группы G, являются управляемые устройства с установленным приложением 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 одного и того же приложения 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. Выключенные профили всегда игнорируются, условия их активации не проверяются.
- 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 Linux управляет работой приложений безопасности "Лаборатории Касперского", установленных на устройствах, путем создания и запуска *задач*. С помощью задач выполняются установка, запуск и остановка приложений, проверка файлов, обновление баз и модулей приложений, другие действия с приложениями.

Вы можете создать задачу для приложения, только если для этого приложения установлен плагин управления.

Задачи могут выполняться на Сервере администрирования и на устройствах.

Задачи, которые выполняются на Сервере администрирования:

- автоматическая рассылка отчетов;
- загрузка обновлений в хранилище Сервера администрирования;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных.

На устройствах выполняются следующие типы задач:

- *Локальные задачи* – это задачи, которые выполняются на конкретном устройстве.

  Локальные задачи могут быть изменены не только администратором средствами Kaspersky Security Center Web Console, но и пользователем удаленного устройства (например, в интерфейсе приложения безопасности). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором, как более приоритетные.

- *Групповые задачи* – это задачи, которые выполняются на всех устройствах указанной группы.

  Если иное не указано в свойствах задачи, групповая задача также распространяется на подгруппы указанной группы. Групповые задачи также действуют (опционально) и на устройства, подключенные к подчиненным и виртуальным Серверам администрирования, размещенным в этой группе и подгруппах.

- *Глобальные задачи* – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.

Для каждого приложения вы можете создавать любое количество групповых задач, глобальных задач и локальных задач.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

Запуск задач на устройстве выполняется только в том случае, если запущено приложение, для которого созданы эти задачи.

Результаты выполнения задач сохраняются в системном журнале событий и журнале событий Kaspersky Security Center Linux 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 **Управление активами → Правила перемещения**.

Правило перемещения по умолчанию предназначено для однократного первоначального размещения устройств в группах администрирования. Правило перемещает нераспределенные устройства только один раз. 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 приложения* или создании автономного инсталляционного пакета.

Можно создать правило перемещения, способное многократно действовать на одно и то же устройство.

Настоятельно рекомендуется избегать подхода к работе с управляемыми устройствами, при котором одно и то же устройство многократно перемещается из группы в группу, например, с целью применения к устройству особой политики, запуска специальной групповой задачи, обновления с определенной точки распространения.

Подобные сценарии не поддерживаются, так как они крайне неэффективны по нагрузке на Сервер администрирования и на сетевой трафик. Также эти сценарии противоречат модели работы Kaspersky Security Center 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 приложений 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 приложений, не подпадающих ни под одну KL-категорию (например, для приложений, разработанных на заказ). Пользовательские категории создаются на основе дистрибутива приложения (MSI) или на основе папки с дистрибутивами.

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 приложения создает задачу резервного копирования параметров Сервера администрирования с ежедневным запуском в четыре часа ночи. Резервные копии по умолчанию сохраняются в папке /var/opt/kaspersky/KSC_Backups*.

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 который выполняется восстановление, должен 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:

- Новому Серверу администрирования должно быть назначено такое же DNS-имя.

  Если при развертывании Агента администрирования в инсталляционном пакете Агента администрирования был задан статический IP-адрес, этот IP-адрес нужно назначить новому Серверу 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).

- В конфигурационном файле IAM `var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` для параметра `server_iam.ksc_address` укажите такой же адрес Сервера администрирования, который указан в альтернативном имени субъекта (SAN) ранее примененного сертификата Сервера администрирования. Подробнее см. в статье Добавление адреса Сервера администрирования в конфигурацию сервера IAM.

- 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.

- Запустите утилиту klbackup и выполните восстановление. Переустановите Web Console после успешного восстановления.

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 распределенного приложения Kaspersky Security Center Linux и, как следствие, неправильная работа приложения.

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.

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.

О переключении Агента администрирования на другой Сервер администрирования

В Kaspersky Security Center Linux предусмотрена возможность переключать Агент администрирования клиентского устройства на другие Серверы администрирования при изменении следующих характеристик сети:

- **Условие для адреса DHCP-сервера** – изменение IP-адреса DHCP-сервера (Dynamic Host Configuration Protocol) в сети.

  Параметр **Условие для адреса DHCP-сервера** в настоящее время недоступен.

- **Условие для адреса шлюза соединения по умолчанию** – изменение основного шлюза сети.
- **Условие для DNS-домена** – изменение DNS-суффикса подсети.
- **Условие для адресов DNS-сервера** – изменение IP-адреса DNS-сервера в сети.
- **Условие для адреса WINS-сервера** – изменение IP-адреса WINS-сервера в сети. Этот параметр доступен только для устройств с операционными системами Windows.
- **Условие для разрешимости имен** – у клиентского устройства изменилось NetBIOS-имя или DNS-имя.
- **Условие для подсети** – изменение адреса и маски подсети.

- **Условие для доступности Windows-домена** – изменение статуса Windows-домена, к которому подключено клиентское устройство. Этот параметр доступен только для устройств с операционными системами Windows.

- **Условие для доступности адреса SSL-соединения** – клиентское устройство может или не может (в зависимости от выбранного вами параметра) установить SSL-соединение с сервером (имя:порт). Используйте выделенный сервер с программным обеспечением, способным обрабатывать высокую нагрузку и частые запросы для подключения от Агента администрирования. Не указывайте порт Сервера администрирования. Для каждого сервера вы можете дополнительно указать SSL-сертификат. В этом случае Агент администрирования проверяет сертификат сервера в дополнение к проверке возможности SSL-соединения. Если сертификаты не совпадают, соединение не устанавливается.

Исходные параметры подключения Агента администрирования к Серверу задаются при установке Агента администрирования. В дальнейшем, если сформированы правила переключения Агента администрирования на другие Серверы администрирования, Агент реагирует на изменение характеристик сети следующим образом:

- Если характеристики сети соответствуют одному из сформированных правил, Агент администрирования подключается к указанному в этом правиле Серверу администрирования. Если это задано правилом, установленные на клиентских устройствах приложения переходят на политики для автономных пользователей.

- Если ни одно из правил не выполняется, Агент администрирования возвращается к исходным параметрам подключения к Серверу администрирования, заданным при установке. Установленные на клиентских устройствах приложения возвращаются к активным политикам.

- Если Сервер администрирования недоступен, Агент администрирования использует политики для автономных пользователей.

Агент администрирования переключается на политику для автономных пользователей, только если параметр **Включить автономный режим, когда Сервер администрирования недоступен** включен в параметрах политики Агента администрирования.

Параметры подключения Агента администрирования к Серверу администрирования сохраняются в профиле подключения. В профиле подключения вы можете создавать правила перехода клиентских устройств на политики для автономных пользователей, а также настраивать профиль таким образом, чтобы он использовался только для загрузки обновлений.

Создание профиля соединения для автономных пользователей

Чтобы создать профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей:

1. Если вы хотите создать профиль подключения для группы управляемых устройств, откройте политику Агента администрирования этой группы. Для этого выполните следующие:

   a. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

   b. Выберите группу администрирования, для которой нужно создать профиль соединения:

      - Для корневой группы вы можете перейти к следующему шагу.

      - Для подгруппы в верхней части страницы нажмите на кнопку **Показать иерархию** и в открывшемся окне нажмите на имя нужной подгруппы.

      Путь к выбранной группе отображается в верхней части страницы. При необходимости вы можете нажать на ссылку с именем группы администрирования, чтобы перейти к группе. По умолчанию последняя ссылка в пути неактивна. Также вы можете закрыть окно иерархии, нажав на кнопку **Скрыть иерархию**.

   c. Добавьте политику Агента администрирования для группы управляемых устройств. Если вы уже создали ее, нажмите на название политики Агента администрирования, чтобы открыть свойства политики.

2. Если вы хотите создать профиль подключения для определенного управляемого устройства, выполните следующие действия:

   a. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.

   b. Нажмите на имя требуемого управляемого устройства.

   c. В открывшемся окне свойств управляемого устройства перейдите на вкладку **Приложения**.

   d. Нажмите на название политики Агента администрирования, к которой применяется только выбранное управляемое устройство.

3. В открывшемся окне свойств перейдите в раздел **Параметры приложения** → **Подключения** → **Профили соединений.**

4. В разделе **Профили подключения к Серверу администрирования** нажмите на кнопку **Добавить**.

   По умолчанию список профилей подключения содержит профили <Офлайн-режим> и <Домашний Сервер администрирования>. Профили недоступны для изменения и удаления.

   В профиле <Офлайн-режим> не указывается Сервер для подключения. При переходе к этому профилю Агент администрирования не пытается подключиться к какому-либо Серверу, а установленные на клиентских устройствах приложения используют политики для автономных пользователей. Профиль <Офлайн-режим> применяется в условиях отключения устройств от сети.

   В профиле <Домашний Сервер администрирования> указан Сервер для подключения, который был задан при установке Агента администрирования. Профиль <Домашний Сервер администрирования> применяется в условиях, когда устройство, которое работало в другой сети, вновь подключается к домашнему Серверу администрирования.

5. В открывшемся окне **Настроить профиль** настройте параметры профиля подключения:

   - **Имя профиля**

     В поле ввода можно просмотреть или изменить имя профиля подключения.

- **Адрес Сервера администрирования**

  Адрес Сервера администрирования, к которому должно подключаться клиентское устройство при активации профиля.

- **Номер порта**

  Номер порта, по которому будет выполняться подключение.

- **SSL-порт**

  Номер порта, по которому будет осуществляться подключение с использованием SSL-протокола.

- **Использовать SSL-соединение**

  Если этот параметр включен, подключение будет выполняться через защищенный порт (с использованием SSL-протокола).

  По умолчанию параметр включен. Чтобы ваше соединение оставалось безопасным, рекомендуется не выключать этот параметр.

- Выберите параметр **Использовать прокси-сервер**, если требуется использовать прокси-сервер для подключения к интернету. Если параметр выбран, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

  - **Адрес**

    Адрес прокси-сервера для подключения Kaspersky Security Center Linux к интернету.

  - **Номер порта**

    Номер порта, через который будет установлено прокси-подключение Kaspersky Security Center Linux.

  - **Аутентификация на прокси-сервере**

    Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  - **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.

- **Адрес шлюза соединения**

  Адрес шлюза, через который устанавливается соединение клиентских устройств с Сервером администрирования.

- **Включить автономный режим, когда Сервер администрирования недоступен**

  Установите этот флажок, чтобы при подключении приложения, установленные на клиентском устройстве, использовали профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей, если Сервер администрирования недоступен. В случае, если для приложения политика для автономных пользователей не определена, приложение будет использовать активную политику.

  Если параметр выключен, приложения будут использовать активные политики.

  По умолчанию флажок снят.

- **Использовать только для получения обновлений**

  Если этот параметр включен, профиль будет использоваться только при загрузке обновлений приложениями, установленными на клиентском устройстве. Для остальных операций подключение к Серверу администрирования будет выполняться с исходными параметрами подключения, заданными при установке Агента администрирования.

  По умолчанию параметр включен.

- **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**

  Если этот параметр включен, Агент администрирования подключается к Серверу администрирования, используя параметры, указанные в свойствах профиля.

  Если этот параметр выключен, Агент администрирования подключается к Серверу, используя исходные параметры, указанные при установке.

  Параметр доступен, если параметр **Использовать только для получения обновлений** выключен.

  По умолчанию параметр выключен.

В результате будет создан профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей. При подключении Агента администрирования к Серверу через этот профиль приложения, установленные на клиентском устройстве, будут использовать политики для устройств, находящиеся в автономном режиме, или политики для автономных пользователей.

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 непрерывную связь 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 управляемому приложению. 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 проверить постоянное соединение управляемого устройства с Сервером администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **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 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 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 сейчас**. Когда Kaspersky Security Center 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.

Руководство по масштабированию

В этом руководстве представлена информация по масштабированию Kaspersky Security Center Linux.

Об этом руководстве

Руководство по масштабированию Kaspersky Security Center Linux (далее также Kaspersky Security Center) адресовано специалистам, которые осуществляют установку и администрирование Kaspersky Security Center, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Security Center.

Все рекомендации и расчеты приведены для сетей, в которых Kaspersky Security Center управляет защитой устройств с установленным программным обеспечением "Лаборатории Касперского".

Для достижения и сохранения оптимальной производительности при различных условиях работы вам нужно учитывать количество устройств в сети, топологию сети и необходимый вам набор функций Kaspersky Security Center.

В руководстве приведена следующая информация:

- Ограничения Kaspersky Security Center.
- Расчеты для ключевых узлов Kaspersky Security Center – Серверов администрирования и точек распространения:
  - Аппаратные требования к Серверам администрирования и к точкам распространения.
  - Расчет количества и иерархии Серверов администрирования.
  - Расчет количества и конфигурации точек распространения.
- Настройка параметров сохранения событий в базе данных в зависимости от числа устройств в сети.
- Общепринятые лучшие практики для оптимизации производительности.
- Настройка параметров некоторых задач для обеспечения оптимальной производительности Kaspersky Security Center.
- Потребление трафика (нагрузка на сеть) между Сервером администрирования Kaspersky Security Center и каждым защищаемым устройством.

Рекомендуется обращаться к этому руководству в следующих ситуациях:

- При планировании ресурсов перед установкой Kaspersky Security Center.
- При планировании существенных изменений размеров сети, в которой развернут Kaspersky Security Center.

- При переходе от использования Kaspersky Security Center в ограниченном сегменте сети (тестовая среда) к полномасштабному развертыванию Kaspersky Security Center в корпоративной сети.
- При изменениях в наборе используемых функций Kaspersky Security Center.

Ограничения Kaspersky Security Center Linux

В таблице ниже приведены ограничения текущей версии Kaspersky Security Center Linux.

Ограничения Kaspersky Security Center Linux

Тип ограничения	Значение
Максимальное количество управляемых устройств на один Сервер администрирования	50 000
Максимальное количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**	300
Максимальное количество групп администрирования	10 000
Максимальное количество хранимых событий	45 000 000
Максимальное количество политик	2000
Максимальное количество задач	2000
Максимальное количество профилей в политике	100
Максимальное количество подчиненных Серверов у одного главного Сервера администрирования	500
Максимальное количество виртуальных Серверов администрирования	500
Максимальное количество устройств, которые может обслуживать одна точка распространения	10 000
Максимальное количество устройств, которые могут использовать один шлюз соединения	10 000, включая мобильные устройства
Максимальное количество мобильных устройств на один Сервер администрирования	100 000 минус количество стационарных управляемых устройств

Расчеты для Серверов администрирования

В этом разделе приведены аппаратные и программные требования для устройств, которые используются в качестве Серверов администрирования. Также даны рекомендации для расчета количества Серверов администрирования и их иерархии, в зависимости от конфигурации сети организации.

Рекомендуется после установки Сервера администрирования и СУБД установить на эти устройства Kaspersky Endpoint Security для Linux. Аппаратные требования для Kaspersky Endpoint Security см. в справке Kaspersky Endpoint Security для Linux.

Нагрузка, создаваемая Kaspersky Endpoint Security для Linux при интеграции с Kaspersky Managed Detection and Response и Kaspersky Endpoint Detection and Response Expert (on-premise), не учитывается в расчетах для совместной установки Kaspersky Security Center Linux и Kaspersky Endpoint Security для Linux.

Расчет аппаратных ресурсов для Сервера администрирования

В этом разделе приведены расчеты, которыми можно руководствоваться при планировании аппаратных ресурсов для Сервера администрирования.

Аппаратные требования для СУБД и Сервера администрирования

В таблицах ниже приведены рекомендуемые минимальные аппаратные требования СУБД и Сервера администрирования, полученные в ходе тестирования. Полный список поддерживаемых операционных систем и СУБД см. в перечне аппаратных и программных требований.

Необходимо включить файл подкачки на устройстве с установленным Сервером администрирования. Минимальный размер файла подкачки должен быть в 1,5 раза больше объема оперативной памяти.

После установки Сервера администрирования и СУБД на устройство рекомендуется установить Kaspersky Endpoint Security для Linux.
Для совместной установки у вас должно быть не менее 300 IOPS, а также нужно добавить к требованиям Сервера администрирования 1,5 ГБ ОЗУ и 15% к требованиям процессора.
Требования к оборудованию для Kaspersky Endpoint Security см. в справке Kaspersky Endpoint Security для Linux.

Информацию о параметрах безопасности, необходимых для работы с Kaspersky Security Center Linux, см. в справке Kaspersky Endpoint Security для Linux.

В сети 50,000 устройств

Конфигурация устройства с Сервером администрирования

Оборудование	Значение
Процессор	8 ядер (рекомендуется 12 ядер), 2500 МГц
ОЗУ	16 ГБ
Дисковое пространство	300 ГБ, 150 IOPS или выше

Конфигурация устройства с установленной СУБД PostgreSQL

Оборудование	Значение
Процессор	16 ядер, 2500 МГц
ОЗУ	32 ГБ
Дисковое пространство	300 ГБ, 150 IOPS или выше

Настройка узлов для отказоустойчивого кластера

Оборудование	Значение
Процессор	8 ядер (рекомендуется 12 ядер), 2500 МГц
ОЗУ	16 ГБ
Дисковое пространство	300 ГБ, 150 IOPS или выше
Контроллер интерфейса сети	1 Гбит/сек

Конфигурация устройства с установленным Сервером администрирования и СУБД PostgreSQL

Оборудование	Значение
Процессор	24 ядра (рекомендуется 28 ядер), 2500 МГц
ОЗУ	48 ГБ
Дисковое пространство	600 ГБ, 300 IOPS или выше

В сети 30 000 устройств

Конфигурация устройства с Сервером администрирования

Оборудование	Значение
Процессор	6 ядер (рекомендуется 8 ядер), 2500 МГц
ОЗУ	12 ГБ
Дисковое пространство	200 ГБ, 150 IOPS или выше

Конфигурация устройства с установленной СУБД PostgreSQL

Оборудование	Значение
Процессор	12 ядер, 2500 МГц
ОЗУ	22 ГБ
Дисковое пространство	250 ГБ, 150 IOPS или выше

Настройка узлов для отказоустойчивого кластера

Оборудование	Значение
Процессор	6 ядер (рекомендуется 8 ядер), 2500 МГц
ОЗУ	12 ГБ
Дисковое пространство	200 ГБ, 150 IOPS или выше
Контроллер интерфейса сети	1 Гбит/сек

Конфигурация устройства с установленным Сервером администрирования и СУБД PostgreSQL

Оборудование	Значение
Процессор	16 ядер (рекомендуется 20 ядер), 2500 МГц
ОЗУ	34 ГБ
Дисковое пространство	450 ГБ, 300 IOPS или выше

В сети 10 000 устройств

Конфигурация устройства с Сервером администрирования

Оборудование	Значение
Процессор	4 ядра (рекомендуется 6 ядер), 2500 МГц
ОЗУ	8 ГБ
Дисковое пространство	100 ГБ, 150 IOPS или выше

Конфигурация устройства с установленной СУБД PostgreSQL

Оборудование	Значение
Процессор	6 ядер, 2500 МГц
ОЗУ	10 ГБ
Дисковое пространство	200 ГБ, 150 IOPS или выше

Настройка узлов для отказоустойчивого кластера

Оборудование	Значение
Процессор	4 ядра (рекомендуется 6 ядер), 2500 МГц
ОЗУ	8 ГБ
Дисковое пространство	100 ГБ, 150 IOPS или выше
Контроллер интерфейса сети	1 Гбит/сек

Конфигурация устройства с установленным Сервером администрирования и СУБД PostgreSQL

Оборудование	Значение
Процессор	8 ядер (рекомендуется 14 ядер), 2500 МГц
ОЗУ	18 ГБ
Дисковое пространство	300 ГБ, 300 IOPS или выше

В сети 1000 устройств

Конфигурация устройства с Сервером администрирования

Оборудование	Значение
Процессор	2 ядра, 2500 МГц
ОЗУ	6 ГБ
Дисковое пространство	10 ГБ, 150 IOPS или выше

Конфигурация устройства с установленной СУБД PostgreSQL

Оборудование	Значение
Процессор	2 ядра, 2500 МГц
ОЗУ	4 ГБ
Дисковое пространство	20 ГБ, 150 IOPS или выше

Настройка узлов для отказоустойчивого кластера

Оборудование	Значение
Процессор	2 ядра, 2500 МГц
ОЗУ	6 ГБ

Оборудование	Значение
Дисковое пространство	10 ГБ, 150 IOPS или выше
Контроллер интерфейса сети	1 Гбит/сек

Конфигурация устройства с установленным Сервером администрирования и СУБД PostgreSQL

Оборудование	Значение
Процессор	4 ядра, 2500 МГц
ОЗУ	10 ГБ
Дисковое пространство	30 ГБ, 300 IOPS или выше

Тестирование проводилось со следующими настройками:

- на Сервере администрирования включено автоматическое назначение точек распространения, либо точки распространения назначены вручную по рекомендуемой таблице;
- СУБД PostgreSQL не включает никаких расширений, кроме plpgsql.

На устройстве, на котором установлена СУБД, база данных занимает примерно 100 ГБ дискового пространства, а журнал транзакций занимает примерно 200 ГБ дискового пространства.

Расчет места в базе данных

Место, которое будет занято в базе данных, можно приблизительно оценить по следующей формуле:

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), КБ,

где:

- "C" – количество устройств.

  > Если в состав управляемых устройств входят динамические виртуальные машины, C – это сумма количества нединамических управляемых устройств и количества динамических виртуальных машин с Агентом администрирования, созданных между двумя последовательными запусками задачи **Обслуживание Сервера администрирования**.

- "E" – количество сохраняемых событий.
- "A" – суммарное количество объектов Active Directory:
  - учетных записей устройств;
  - учетных записей пользователей;
  - учетных записей групп безопасности;
  - подразделений Active Directory.

  Если сканирование Active Directory выключено, то "A" следует считать равным нулю.

- N – среднее количество инвентаризируемых исполняемых файлов на конечном устройстве.
- F – количество конечных устройств, на которых были инвентаризированы исполняемые файлы.

Если вы планируете включить в параметрах политики Kaspersky Endpoint Security информирование Сервера администрирования о запускаемых приложениях, то для хранения информации о запускаемых приложениях в базе данных дополнительно потребуется (0,03 * C) ГБ.

В ходе работы в базе данных всегда образуется так называемое *незанятое пространство* (unallocated space). Поэтому фактический размер файла базы данных часто оказывается примерно в два раза больше, чем объем пространства, занимаемого в базе данных.

Не рекомендуется явным образом ограничивать размер журнала транзакций. Рекомендуется оставить значение параметра MAXSIZE по умолчанию.

Расчет места на диске

Место на диске Сервера администрирования, требуемое для папки /var/opt/kaspersky/klnagent_srv/, можно приблизительно оценить по формуле:

(724 * C + 0.15 * E + 0.17 * A), КБ

где:

- "C" – количество устройств.

  Если в состав управляемых устройств входят динамические виртуальные машины, C – это сумма количества нединамических управляемых устройств и количества динамических виртуальных машин с Агентом администрирования, созданных между двумя последовательными запусками задачи **Обслуживание Сервера администрирования**.

- "E" – количество сохраняемых событий.
- "A" – суммарное количество объектов Active Directory:
  - учетных записей устройств;
  - учетных записей пользователей;
  - учетных записей групп безопасности;
  - подразделений Active Directory.

Если сканирование Active Directory выключено, то "A" следует считать равным нулю.

Расчет количества и конфигурации Серверов администрирования

Чтобы снизить нагрузку на главный Сервер администрирования, вы можете назначить в каждую группу администрирования отдельный Сервер администрирования. Количество Серверов администрирования, подчиненных главному Серверу, не может превышать 500.

Рекомендуется выстраивать конфигурацию Серверов администрирования в зависимости от того, как настроена сеть в вашей организации.

Рекомендации по подключению динамических виртуальных машин к Kaspersky Security Center

Динамические виртуальные машины потребляют больше ресурсов, чем статические виртуальные машины.

Дополнительные сведения о динамических виртуальных машинах см. Поддержка динамических виртуальных машин.

При подключении новой динамической виртуальной машины Kaspersky Security Center Linux создает запись этой динамической виртуальной машины в Kaspersky Security Center Web Console и перемещает динамическую виртуальную машину в группу администрирования. После этого динамическая виртуальная машина добавляется в базу данных Сервера администрирования. Сервер администрирования полностью синхронизирован с Агентом администрирования, установленным на этой динамической виртуальной машине.

В сети организации Агент администрирования создает для каждой динамической виртуальной машины следующие сетевые списки:

- оборудование;
- установленное программное обеспечение;
- обнаруженные уязвимости;
- события и списки исполняемых файлов компонента Контроль приложений.

Агент администрирования передает эти сетевые списки на Сервер администрирования. Размер сетевых списков зависит от компонентов, установленных на динамической виртуальной машине, и может влиять на производительность Kaspersky Security Center Linux и системы управления базами данных (СУБД). Обратите внимание, что нагрузка может расти нелинейно.

После того, как пользователь заканчивает работу с динамической виртуальной машиной и выключает ее, эта машина удаляется из виртуальной инфраструктуры, записи о ней удаляются из базы данных Сервера администрирования.

Все эти действия используют много ресурсов базы данных Kaspersky Security Center Linux и Сервера администрирования и могут снизить производительность Kaspersky Security Center Linux и СУБД. Рекомендуется подключать к Kaspersky Security Center Linux до 20 000 динамических виртуальных машин.

Вы можете подключить к Kaspersky Security Center Linux более 20 000 динамических виртуальных машин, если подключенные динамические виртуальные машины выполняют стандартные операции (например, обновление баз) и потребляют не более 80% памяти и 75–80% доступных ядер.

Изменение параметров политики, программного обеспечения или операционной системы на динамической виртуальной машине может уменьшить или увеличить потребление ресурсов. Оптимальным считается потребление 80–95% ресурсов.

Расчеты для точек распространения и шлюзов соединений

В этом разделе приведены аппаратные требования к устройствам, которые используются в качестве точек распространения, и рекомендации по расчету количества точек распространения и шлюзов соединений в зависимости от конфигурации сети организации.

Требования для точки распространения

Аппаратные и программные требования для точек распространения под управлением Windows и Linux описаны в этой статье.

При наличии на Сервере администрирования задач удаленной установки, на устройстве с точкой распространения дополнительно потребуется дисковое пространство, равное суммарному размеру устанавливаемых инсталляционных пакетов.

При наличии на Сервере администрирования одного или нескольких экземпляров задачи установки обновлений (патчей) и закрытия уязвимостей на устройстве с точкой распространения дополнительно потребуется дисковое пространство, равное удвоенному суммарному размеру всех устанавливаемых патчей.

Если вы используете схему, по которой точки распространения получают обновления баз и модулей приложений напрямую с серверов обновлений "Лаборатории Касперского", точки распространения должны быть подключены к сети интернет.

Не рекомендуется назначать Сервер администрирования в качестве точки распространения, так как это увеличит нагрузку на Сервер администрирования.

Аппаратные требования для точек распространения под управлением Windows

Минимальные аппаратные требования для точек распространения под управлением Windows

Количество клиентских устройств	процессор;	оперативная память;	Объем оперативной памяти, с включенным управлением исправлениями	Дисковое пространство
10 000	4 ядра, 2500 МГц	8 ГБ	8 ГБ	120 ГБ

5000	4 ядра, 2500 МГц	6 ГБ	8 ГБ	120 ГБ
1000	2 ядра, 2500 МГц	4 ГБ	8 ГБ	120 ГБ

Аппаратные требования для точек распространения под управлением Linux

Минимальные аппаратные требования для точек распространения под управлением Linux

Количество клиентских устройств	процессор;	оперативная память;	Дисковое пространство
10 000	4 ядра, 2500 МГц	10 ГБ	120 ГБ
5000	4 ядра, 2500 МГц	8 ГБ	120 ГБ
1000	2 ядра, 2500 МГц	6 ГБ	120 ГБ

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 специально выделенных точек распространения в сети, содержащей один сегмент сети, в зависимости от количества устройств в сети

Число клиентских устройств в сегменте 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 специально выделенных точек распространения в сети, содержащей несколько сегментов сети, в зависимости от количества устройств в сети

Число клиентских устройств в каждом 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 сегменте 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 каждом 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.

Расчет количества шлюзов соединений

Если вы планируете использовать шлюз соединений, рекомендуется использовать выделенное устройство для этой функции.

Один шлюз соединений обслуживает не более 10 000 управляемых устройств.

Хранение информации о событиях для задач и политик

В этом разделе приведены расчеты, связанные с хранением событий в базе данных Сервера администрирования, и даны рекомендации, как минимизировать количество событий и таким образом снизить нагрузку на Сервер администрирования.

По умолчанию в свойствах каждой задачи и каждой политики указано сохранение в журнале всех событий, связанных с выполнением задачи и применением политики.

Однако если задача запускается достаточно часто (например, более одного раза в неделю) и на достаточно большом количестве устройств (например, более 10 000), количество событий может оказаться слишком большим, и события могут заполнить базу данных. В таком случае рекомендуется указать в свойствах задачи один из двух других вариантов:

- **Сохранять события, связанные с ходом выполнения задачи**. В этом случае с каждого устройства, на котором выполнена задача, в базу данных поступает только информация о запуске задачи, о ее ходе и о ее выполнении (успешном, с предупреждением либо с ошибкой).

- **Сохранять только результат выполнения задачи**. В этом случае с каждого устройства, на котором выполнена задача, в базу данных поступает только информация о выполнении задачи (успешном, с предупреждением либо с ошибкой).

Если политика определена для достаточно большого количества устройств (например, более 10 000), количество событий также может оказаться слишком большим, и события могут заполнить базу данных. В таком случае рекомендуется выбрать в свойствах политики только наиболее важные события и включить их сохранение. Сохранение всех других событий рекомендуется отключить.

Таким образом вы уменьшаете количество событий в базе данных, увеличиваете скорость работы сценариев, связанных с анализом таблицы событий в базе данных, и снижаете риск вытеснения критических событий большим количеством событий.

Вы также можете уменьшить срок хранения событий, связанных с задачей или политикой. По умолчанию этот срок составляет семь дней для событий, связанных с задачей, и 30 дней для событий, связанных с политикой. При изменении срока хранения событий принимайте в расчет порядок работы, принятый в вашей организации, и количество времени, которое системный администратор может уделять анализу каждого события.

Вносить изменения в параметры хранения событий целесообразно в любом из следующих случаев:

- события об изменении промежуточных состояний групповых задач и о применении политик занимают значительный процент всех событий в базе данных Kaspersky Security Center Linux;

- в журнале событий операционной системы появляются записи об автоматическом удалении событий при превышения заданного лимита на общее число событий, хранимых в базе данных.

Выберите параметры регистрации событий, исходя из того, что оптимальное количество событий, поступающих с одного устройства в день, не должно превышать 20. Вы можете немного увеличить максимальное количество событий, если это необходимо, но только в том случае, если количество устройств в вашей сети относительно невелико (менее 10 000).

Лучшие практики для Сервера администрирования, управляющего большим количеством устройств

Лучшие практики использования СУБД

Настройте регулярное выполнение задачи **Обслуживание Сервера администрирования**, особенно если вы используете СУБД PostgreSQL.

Исключите папку СУБД из проверки IOC.

Лучшие практики для политик и профилей политик

Уменьшите количество активных политик для компонента (например, Kaspersky Endpoint Security для Windows). Вы можете заменить политики профилями политик.

Лучшие практики для Сервера администрирования, управляющего большим количеством устройств

Уменьшите количество одновременно выполняемых задач, особенно задач удаленной установки и управления патчами.

Уменьшите количество задач и оптимизируйте расписание задач, работающих с выборками устройств.

В разделе параметров политики **Настройка событий** уменьшите количество сохраняемых типов событий.

Лучшие практики хранения событий

Уменьшите частоту однотипных событий от компонента Контроль приложений. Дополнительную информацию см. в статье О блокировке частых событий.

Уменьшите срок хранения событий компонентов (например, Kaspersky Endpoint Security для Windows) и информационных событий о закрытии уязвимостей.

Включите параметр **Сохранять события, связанные с ходом выполнения задачи** в свойствах задачи для общих задач, таких как задачи обновления. Подробнее см. в статье Хранение информации о событиях для задач и политик.

Оптимизируйте параметры задачи инвентаризации. Дополнительную информацию см. в статье Задача инвентаризации.

Особенности и оптимальные параметры некоторых задач

Некоторые задачи имеют особенности, связанные с количеством устройств в сети. В этом разделе даны рекомендации по оптимальной настройке параметров для таких задач.

Обнаружение устройств, задача резервного копирования данных, задача обслуживания базы данных и групповые задачи обновления Kaspersky Endpoint Security входят в базовую функциональность Kaspersky Security Center Linux.

Задача инвентаризации входит в возможность Системного администрирования и недоступна, если эта возможность не активирована.

Частота обнаружения устройств

Не рекомендуется увеличивать установленную по умолчанию частоту поиска устройств, так как это может создать чрезмерную нагрузку на контроллеры домена. Рекомендуется, наоборот, устанавливать расписание опроса с минимально возможной частотой, насколько позволяют потребности вашей организации. В таблице ниже приведены рекомендации по расчету оптимального расписания.

Расписание обнаружения устройств

Количество устройств в сети	Рекомендуемая частота для обнаружения устройств
Менее 10 000	Установленная по умолчанию или реже
10 000 и более	Один раз в сутки или реже

Задачи резервного копирования данных Сервера администрирования и обслуживания базы данных

Сервер администрирования перестает функционировать во время выполнения следующих задач:

- Резервное копирование данных Сервера администрирования
- Обслуживание Сервера администрирования

Пока выполняются эти задачи, данные не могут поступать в базу данных.

Вам может потребоваться изменить расписание этих задач так, чтобы их выполнение не пересекалось по времени с выполнением других задач Сервера администрирования.

Групповые задачи обновления Kaspersky Endpoint Security

Если источником обновлений является Сервер администрирования, то для групповых задач обновления Kaspersky Endpoint Security версии 10 и выше рекомендуется расписание **При загрузке обновлений в хранилище** с установленным флажком **Автоматически определять интервал для распределения запуска задачи**.

Если вы создали на каждой точке распространения локальную задачу загрузки обновлений в хранилище с серверов "Лаборатории Касперского", то для групповой задачи обновления Kaspersky Endpoint Security рекомендуется задать периодическое расписание. Значение периода автономизации в этом случае должно составлять один час.

Задача Инвентаризации

Вы можете снизить нагрузку на базу данных при получении информации об исполняемых файлах. Для этого рекомендуется запускать задачу инвентаризации для Kaspersky Endpoint Security на нескольких эталонных устройствах, на которых установлен стандартный набор приложений.

Количество исполняемых файлов, получаемых Сервером администрирования от одного устройства, не может превышать 150 000. При достижении этого ограничения Kaspersky Security Center Linux не получит новые файлы.

Количество файлов на обыкновенном клиентском устройстве, как правило, составляет не более 60 000. Количество исполняемых файлов на файловом сервере может быть больше и может даже превышать порог в 150 000.

Информация о нагрузке на сеть между Сервером администрирования и защищаемыми устройствами

В этом разделе приводятся результаты тестовых замеров трафика в сети с указанием условий, при которых проводились замеры. Вы можете использовать эту информацию как справочную при планировании сетевой инфраструктуры и пропускной способности каналов внутри организации (либо между Сервером администрирования и организацией, в которой расположены защищаемые устройства). Зная пропускную способность сети, вы также можете приблизительно оценивать, сколько времени должна занять та или иная операция, связанная с передачей данных.

Потребление трафика при выполнении различных сценариев

В таблице ниже приводятся результаты тестовых замеров трафика между Сервером администрирования и управляемым устройством при выполнении различных сценариев.

Синхронизация устройства с Сервером администрирования происходит по умолчанию раз в 15 минут либо реже. Однако если вы меняете на Сервере администрирования параметры политики или задачи, то происходит досрочная синхронизация устройств, для которых применима эта политика (или задача), и новые параметры передаются на устройства.

Трафик между Сервером администрирования и управляемым устройством

Сценарий	Трафик от Сервера к каждому управляемому устройству	Трафик от каждого управляемого устройства к Серверу
Установка Kaspersky Endpoint Security для Linux с обновленными базами	390 МБ	3.3 МБ
Установка Агента администрирования	75 МБ	397 КБ
Совместная установка Агента администрирования и Kaspersky Endpoint Security для Linux	459 МБ	3.6 МБ
Первоначальное обновление антивирусных баз без обновления баз в пакете (если участие в Kaspersky Security Network выключено)	113 МБ	1,8 МБ
Ежесуточное обновление антивирусных баз (если участие в Kaspersky Security Network включено)	22 МБ	373 МБ
Первоначальная синхронизация до обновления баз на устройстве (передача политик и задач)	382 КБ	446 КБ
Первоначальная синхронизация после обновления баз на устройстве	20 КБ	157 КБ
Синхронизация при отсутствии изменений на Сервере администрирования (по расписанию)	18 КБ	23 КБ
Синхронизация при изменении одного параметра в политике группы (досрочная, сразу после внесения изменения)	19 КБ	20 КБ

Сценарий	Трафик от Сервера к каждому управляемому устройству	Трафик от каждого управляемого устройства к Серверу
Синхронизация при изменении одного параметра в групповой задаче (досрочная, сразу после внесения изменения)	14 КБ	11 КБ
Принудительная синхронизация	110 КБ	109 КБ
Событие **Обнаружен вирус** (1 вирус)	44 КБ	50 КБ
Событие **Обнаружен вирус** (10 вирусов)	58 КБ	77 КБ
Разовый трафик после включения списка реестра приложений	до 10 КБ	до 12 КБ
Ежедневный трафик при включенном списке реестра приложений	до 840 КБ	до 1 МБ

Средний расход трафика за сутки

Средний расход трафика за сутки между Сервером администрирования и управляемым устройством:

- Трафик от Сервера к управляемому устройству – 840 КБ.
- Трафик от управляемого устройства к Серверу – 1 МБ.

Трафик был измерен при следующих условиях:

- На управляемом устройстве были установлены Агент администрирования и Kaspersky Endpoint Security для Linux.
- Устройство не было назначено точкой распространения.
- Системное администрирование не было включено.
- Период синхронизации с Сервером администрирования составляло 15 минут.

Известные проблемы и ограничения

Kaspersky Security Center Linux имеет следующие ограничения, не критичные для работы приложения:

- 8698100: Задача **Резервное копирование данных Сервера администрирования** завершается с ошибкой "Убедитесь, что SQL-сервер имеет доступ к папке назначения" при использовании двухсторонней аутентификации между утилитой klpg_dump и PostgreSQL.
- 10253149: В свойствах политики Kaspersky Endpoint Security для Windows (**Настройка событий** → **Предупреждения**) при переходе в свойства типа события **Задача остановлена** не отображается раскрывающийся текст о признаке массовости события.
- 10723777: При обновлении баз с помощью задачи **Загрузка обновлений в хранилище Сервера администрирования** Kaspersky Security Center Linux пытается использовать базы с локализацией, отличающейся от локализации Kaspersky Security Center Linux, если используется не английская (en) локализация.
- 10427694: На Ubuntu 24.04 из-за проблем с обработкой асинхронных обращений к системным функциям Сервер администрирования ошибочно генерирует дампы.
- 10007954: После создания и запуска задачи **Поиск уязвимостей и требуемых обновлений** при переходе в результаты выполнения задачи на подчиненном Сервере появляется ошибка "Соединение с Сервером администрирования прервано".
- 10671377: При использовании PostgreSQL и Postgres Pro версий 18.1-18.5 запущенные задачи могут завершаться с ошибкой "'[53000]' ERROR: no empty local buffer available". Рекомендуется обновить PostgreSQL до версии 18.6, либо выполнить следующие действия:

  1. Остановите службу Сервера администрирования.
  2. Остановите службу СУБД.
  3. В конец файла postgresql.conf добавьте следующую строку: `effective_io_concurrency=0`.
  4. Запустите службу СУБД.
  5. Убедитесь, что значение параметра `effective_io_concurrency` равно `0` с помощью следующего запроса:

     ```
     SELECT setting FROM pg_settings WHERE name = 'effective_io_concurrency';
     ```

  6. Запустите службу Сервера администрирования.
- 10564198: При обновлении Kaspersky Security Center Linux до версии 16.3 на узлах отказоустойчивого кластера Kaspersky Security Center Linux запуск скрипта postinstall.pl для настройки Сервера администрирования может привести к ошибкам установки.
- 8994760: Если у вас есть права доступа к виртуальным Серверам администрирования, но нет прав доступа к главному Серверу администрирования, и вы пытаетесь выполнить вход в Kaspersky Security Center Linux, возникает ошибка, при этом отображается сообщение об ошибке **Ваш запрос в настоящее время не может быть обработан. Пожалуйста, подождите и попробуйте позже**, которое является некорректным. Текст ошибки должен быть следующим: **Проверьте свои права доступа. У вас должны быть права доступа на главном Сервере или только на одном из виртуальных Серверов. Свяжитесь с главным администратором и повторите попытку**

- 10302954: При задании условий правила перемещения устройства, если на вкладке **Сеть** включить параметр **Устройство находится в подгруппе группы "Домены"**, раскрывающийся список подгрупп отображается пустым.

- 10253149: Для политик приложений, если на вкладке **Настройка событий** вы выбрали массовое событие, раскрывающийся блок **Подробнее** с предупреждением о влиянии таких событий на Сервер администрирования или производительность СУБД не отображается.

- 9302142: Параметр **Использовать в качестве шлюза соединения в демилитаризованной зоне** не поддерживается для Microsoft Windows на Arm.

- 9065814: Ошибка может возникнуть при попытке доменной аутентификации с устройства под управлением Windows в домене Samba 4.

- 9335676: После переключения управляющего узла в кластере СУБД высокой доступности доступ к Kaspersky Security Center Web Console может быть недоступен или значительно задержан. Если Kaspersky Security Center Web Console остается недоступным более 10 минут, перезапустите службу IAM с помощью следующей команды:

  ```
  systemctl restart kliam_srv.service
  ```

- 9157005, 9157085: При запуске задачи *Установка требуемых обновлений и закрытие уязвимостей* с включенным параметром **Начинать установку в момент перезагрузки или выключения устройства** на управляемом устройстве с операционной системой Windows задача может завершиться ошибкой. Эта проблема может возникнуть, если запланирована установка большого количества обновлений. Чтобы решить эту проблему запустите задачу, выключив параметр **Начинать установку в момент перезагрузки или выключения устройства**.

- 9272534: Если таблица пользователей содержит более 50 000 пользователей, отображаются только первые 50 000 пользователей, остальные пользователи не отображаются.

- 9291235: После восстановления из резервной копии на Сервере администрирования версии 16.1 в Kaspersky Security Center Web Console отображается страница входа в систему. После успешной аутентификации запрашивается одноразовый код безопасности для двухфакторной аутентификации. Несмотря на ввод действительного одноразового кода безопасности, отображается сообщение об ошибке, указывающее на то, что одноразовый код безопасности неверен. В этом случае следует подождать несколько минут, а затем вручную обновить страницу и повторить попытку входа в Kaspersky Security Center Web Console. После того, как процесс восстановления резервной копии будет полностью завершен, следующая попытка аутентификации будет успешной.

- 7939561: При попытке изменить защищенную учетную запись пользователя, нажав на кнопку **Отмена** в окне ввода учетных данных **Защита учетной записи** отображается ошибка.

- 8562938: При открытии порта для мобильных устройств в свойствах политики Сервера администрирования функция управления мобильными устройствами не включается и мобильный сертификат не генерируется. Чтобы включить функцию управления мобильными устройствами, в свойствах Сервера администрирования должен быть открыт порт для мобильных устройств.

- 8732282: Для пользователя, для которого в свойствах учетной записи в Active Directory включен параметр **Пользователь не может изменить пароль**, действие **Сбросить пароль** в Active Directory выполняться не будет. Администратору контроллера домена нужно либо выключить параметр **Пользователь не может изменить пароль** для этого пользователя, либо сбросить пароль вручную. Эта проблема возникает, если у вас есть лицензия Kaspersky Security для бизнеса Профессиональный, включена интеграция с Active Directory и пользователь включен в группу безопасности Active Directory.

- 8688182: Если в свойствах учетной записи в Active Directory для пользователя включен параметр **Срок действия пароля не ограничен**, после выполнения действия **Сбросить пароль** параметр **Срок действия пароля не ограничен** будет выключен и пользователю потребуется изменить доменный пароль при следующем входе в систему. Эта проблема возникает, если у вас есть лицензия Kaspersky Security для бизнеса Профессиональный, включена интеграция с Active Directory и пользователь включен в группу безопасности Active Directory.

- 8703857: Подключение к прокси-серверу для Kaspersky Security Center Web Console и веб-плагинов управления устанавливается только в том случае, если прокси-сервер поддерживает базовую аутентификацию.

- 7911778: При запуске задачи **Удаленная деинсталляция приложения** для удаления Агента администрирования с устройства, на котором работает операционная система с архитектурой Arm и которое также имеет несинхронизированное время с Сервером администрирования, статус задачи не меняется с **Выполняется** на **Завершена**, даже после успешного удаления Агента администрирования с устройства. Чтобы решить эту проблему, синхронизируйте время на устройстве с установленным Агентом администрирования с устройством с Сервером администрирования перед запуском задачи **Удаленная деинсталляция приложения**.

- 6896585: Управляемое устройство не может подключиться к KSN через службу прокси-сервер KSN, если Kaspersky Security Center Linux установлен на устройстве, имя которого содержит кириллические символы.

- 7523299: Агент администрирования не перезагружается после завершения работы своего процесса на управляемом устройстве под управлением CentOS 6.6.

- 7835858: Если вы создаете задачу с **параметрами расписания Каждые N дней** и По дням недели в Kaspersky Security Center Web Console версии 15.2 и выше, а затем открываете задачу в более ранних версиях Kaspersky Security Center Web Console или Консоли администрирования (например, когда задача также применяется на подчиненных Серверах администрирования, которые могут быть как с операционной системой Linux, так и с Windows), параметры расписания могут отображаться некорректно или может произойти ошибка.

- 7208621: При импорте задачи *Загрузить обновления в хранилища точек распространения* или задачи *Проверка обновлений* параметр **Выбор устройств, которым будет назначена задача** включен. Эти задачи невозможно назначить выборкам устройств или заданным устройствам. Если вы назначите задачу *Загрузить обновления в хранилища точек распространения* или задачу *Проверка обновлений* на определенные устройства, задача будет импортирована некорректно.

- 6511063: Если на устройстве с операционной системной Linux обнаружено приложение из раздела **Реестр приложений**, в свойствах приложения отсутствует информация о связанных с ним исполняемых файлах.

- 5915107: В отчетах с буквенным форматом разрыв страницы может обрезать строку текста по горизонтали.

- 5556109: 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.

- 9093038: Если Сервер администрирования Kaspersky Security Center Linux не запускается после установки и журнал событий операционной системы содержит ошибку 213/SECUREBITS, связанную со службой kladminserver_srv.service, выполните от имени суперпользователя следующие команды:

```
mkdir -p /etc/systemd/system/kladminserver_srv.service.d
echo "[Service]" > /etc/systemd/system/kladminserver_srv.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kladminserver_srv.service.d/override.conf
mkdir -p /etc/systemd/system/klwebsrv_srv.service.d
echo "[Service]" > /etc/systemd/system/klwebsrv_srv.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/klwebsrv_srv.service.d/override.conf
```

  Если Kaspersky Security Center Web Console не запускается после установки и журнал событий операционной системы содержит ошибку 213/SECUREBITS, связанную со службой KSCWebConsole.service, выполните от имени суперпользователя следующие команды:

```
mkdir -p /etc/systemd/system/KSCSvcWebConsole.service.d
echo "[Service]" > /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsoleManagement.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsoleNATS.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsolePlugin.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsole.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsole.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsole.service.d/override.conf
```

  Если служба kliam_srv не запускается после установки, а журнал операционной системы содержит ошибку 213/SECUREBITS, связанную с этой службой, выполните следующие команды от имени суперпользователя:

```
mkdir -p /etc/systemd/system/kliam_srv.service.d
echo "[Service]" > /etc/systemd/system/kliam_srv.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kliam_srv.service.d/override.conf
```

- 9165434: NTLM-аутентификация не работает для учетных записей пользователей группы "Защищенные пользователи".

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 вашей проблемы в документации или других источниках информации о Kaspersky Security Center Linux, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Security Center.

Kaspersky предоставляет поддержку Kaspersky Security Center в течение жизненного цикла (см. страницу жизненного цикла приложений). 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 сайт Службы технической поддержки;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;

- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки.

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 Linux, 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 приложении

Страница Kaspersky Security Center Linux на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Security Center Linux вы можете получить общую информацию о приложении, его возможностях и особенностях работы.

Страница Kaspersky Security Center Linux 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 Linux и с другими приложениями "Лаборатории Касперского". Также в статьях Базы знаний могут быть новости Службы технической поддержки.

Обсуждение приложений "Лаборатории Касперского" в сообществе пользователей

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем Форуме.

На Форуме 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.

Глоссарий

Cloud discovery

Cloud Discovery управляет доступом пользователей к облачным сервисам. К облачным сервисам относятся, например, Microsoft Teams, Salesforce, Microsoft Office 365. Облачные сервисы сгруппированы в категории, например, категории *Файловые обменники*, *Мессенджеры*, *Электронная почта*.

FileTransferBridge

Внутренний компонент Kaspersky Security Center Linux, который обеспечивает локальную доставку обновлений приложений "Лаборатории Касперского". FileTransferBridge интегрирован в Агент администрирования (klnagent) и запускается локально на каждом управляемом устройстве.

Когда приложения "Лаборатории Касперского" получают обновления от Kaspersky Security Center Linux, Агент администрирования загружает файлы обновлений с Сервера администрирования или с точки распространения. Затем FileTransferBridge передает файлы локально установленным приложениям "Лаборатории Касперского", обеспечивая надежную доставку обновлений баз данных и патчей.

FileTransferBridge использует TCP-порты 30522 и 30523. Порты прослушивают только интерфейс localhost (127.0.0.1) и не принимают входящие подключения из внешних сетей.

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.

Identity and Access Manager (IAM)

Компонент Сервера администрирования, позволяющий использовать доменную аутентификацию (единый вход). Функция единого входа позволяет пользователю включить безопасную аутентификацию в Kaspersky Security Center Web Console без повторного ввода пароля в корпоративной сети.

iOS MDM-устройство

Мобильное устройство, которое подключается к Серверу iOS MDM по протоколу iOS MDM. По протоколу iOS MDM могут подключаться и управляться устройства с операционной системой iOS.

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 Security Center Linux System Health Validator (SHV)

Компонент приложения Kaspersky Security Center Linux, предназначенный для проверки работоспособности операционной системы при совместной работе приложения Kaspersky Security Center Linux с Microsoft NAP.

Lightweight Nagent (LWNGT)

Протокол взаимодействия с Kaspersky Endpoint Security на мобильных устройствах. Протокол LWNGT (также мобильный протокол) выполняет роль Агента администрирования без фактической установки Агента администрирования на мобильные устройства.

Network Location Awareness (NLA)

Служба Windows, которая помогает операционной системе идентифицировать текущую сеть. NLA обнаруживает изменения в сети и настраивает конфигурацию безопасности устройства.

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 приложений Kaspersky Security Center Linux, осуществляющий взаимодействие между Сервером администрирования и приложениями "Лаборатории Касперского", установленными на конкретном сетевом узле (рабочей станции или сервере). Этот компонент является единым для всех приложений компании для Windows. Для приложений "Лаборатории Касперского" для Novell®, Unix™ и Mac 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.

Агент обновлений

Устройство с установленным Агентом администрирования, которое используется для распространения обновлений, удаленной установки приложений, получения информации об устройствах в составе группы администрирования и/или широковещательного домена. Агенты обновлений предназначены для уменьшения нагрузки на Сервер администрирования при распространении обновлений и для оптимизации трафика в сети. Агенты обновлений могут быть назначены автоматически Сервером администрирования или вручную администратором.

Административные права

Уровень прав и полномочий пользователя для администрирования объектов Exchange внутри организации Exchange.

Администратор Kaspersky Security Center Linux

Лицо, управляющее работой приложения через систему удаленного централизованного администрирования Kaspersky Security Center Linux.

Администратор клиента

Сотрудник организации-клиента, который отвечает за обеспечение антивирусной безопасности 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 приложения.

Антивирусная безопасность сети

Комплекс технических и организационных мер, снижающих вероятность проникновения на устройства сети организации вирусов и спама, предотвращающих сетевые атаки, фишинг и другие угрозы. Антивирусная безопасность сети повышается при использовании приложений защиты 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 Linux

Компонент Kaspersky Security Center Linux, который устанавливается в составе Сервера администрирования. Веб-сервер предназначен для передачи по сети автономных пакетов установки, iOS MDM-профилей, а также файлов из папки общего доступа.

Виртуальный Сервер администрирования

Компонент приложения Kaspersky Security Center Linux, 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).

Вирусная атака

Ряд целенаправленных попыток заразить устройство вирусом.

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. Под именем учетной записи внутреннего пользователя администратор виртуального Сервера может запускать Kaspersky Security Center Web Console для просмотра сведений о состоянии антивирусной безопасности сети. В рамках функциональности приложения Kaspersky Security Center Linux внутренние пользователи обладают правами реальных пользователей.

Учетные записи внутренних пользователей создаются и используются только внутри Kaspersky Security Center Linux. Сведения о внутренних пользователях не передаются операционной системе. Аутентификацию внутренних пользователей осуществляет Kaspersky Security Center Linux.

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:

- информационную базу Сервера администрирования (политики, задачи, параметры приложения, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов приложений для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором приложений "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждого из установленных в группе приложений могут быть созданы групповые политики и сформированы групповые задачи.

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 ключ

Ключ, подтверждающий право на использование приложения, но не используемый в текущий момент.

Доступное обновление

Пакет обновлений модулей приложения "Лаборатории Касперского", в состав которого включены набор срочных обновлений, собранных за некоторый период, и изменения в архитектуре приложения.

Задача

Функции, выполняемые приложением "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 приложения "Лаборатории Касперского" при помощи системы удаленного управления Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки приложения и обеспечения его работоспособности сразу после установки. Значения параметров соответствуют значениям параметров приложения по умолчанию. Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива приложения.

Клиент Сервера администрирования (Клиентское устройство)

Устройство, сервер или рабочая станция, на котором установлены Агент администрирования и управляемые приложения "Лаборатории Касперского".

Консоль администрирования

Компонент приложения Kaspersky Security Center Linux, предоставляющий пользовательский интерфейс к административным службам Сервера администрирования и Агента администрирования.

Конфигурационный профиль

Политика, содержащая набор параметров и ограничений для мобильного устройства iOS MDM.

Локальная задача

Задача, определенная и выполняющаяся на отдельном клиентском устройстве.

Локальная установка

Установка приложения защиты на устройство сети организации, которая предусматривает ручной запуск установки из дистрибутива приложения защиты или ручной запуск опубликованного инсталляционного пакета, предварительно загруженного на устройство.

Магазин приложений

Компонент приложения Kaspersky Security Center Linux. 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.

Настройки задачи

Настройки работы приложения, специфичные для каждого типа задач.

Непосредственное управление приложением

Управление приложением через локальный интерфейс.

Несовместимое приложение

Антивирусное приложение стороннего производителя или приложение "Лаборатории Касперского", не поддерживающее управление через Kaspersky Security Center Linux.

Обновление

Процедура замены / 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 приложения

Параметры работы приложения, общие для всех типов его задач и отвечающие за работу приложения в целом, например: параметры производительности приложения, параметры ведения отчетов, параметры резервного хранилища.

Политика

Политика определяет параметры работы приложения и доступ к настройке приложения, установленного на устройствах группы администрирования. Для каждого приложения требуется создать свою политику. Вы можете создать неограниченное количество различных политик для приложений, установленных на устройствах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждому приложению.

Поставщик услуг антивирусной защиты

Организация, предоставляющая услуги антивирусной защиты сетей организации-клиента на основе решений "Лаборатории Касперского".

Профиль

Набор параметров поведения мобильных устройств Exchange ActiveSync при подключении к серверу Microsoft Exchange.

Рабочее место администратора

Устройство, на котором установлена Консоль администрирования – компонент, предоставляющий интерфейс управления Kaspersky Security Center Linux.

С рабочего места администратор управляет серверной частью Kaspersky Security Center: выстраивает систему централизованной защиты сети организации, сформированную на базе приложений "Лаборатории Касперского", и контролирует ее.

Резервное копирование данных Сервера администрирования

Копирование данных Сервера администрирования для резервного хранения и последующего восстановления, осуществляемое при помощи утилиты резервного копирования. Утилита позволяет сохранять:

- информационную базу Сервера администрирования (политики, задачи, параметры приложения, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов приложений для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

Ролевая группа

Группа пользователей мобильных устройств Exchange ActiveSync, которые обладают одинаковыми административными правами.

Ручная установка

Установка приложения защиты на устройство сети организации из дистрибутива приложения защиты. Ручная установка требует непосредственного участия администратора или другого IT-специалиста. Обычно ручная установка применяется, если удаленная установка завершилась с ошибкой.

Сервер iOS MDM

Компонент Kaspersky Security Center, который устанавливается на клиентское устройство и позволяет подключать мобильные устройства iOS к Серверу администрирования и управлять ими с помощью сервиса Apple Push Notifications (APNs).

Сервер администрирования

Компонент приложения Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации приложениях "Лаборатории Касперского" и управления ими.

Серверы обновлений "Лаборатории Касперского"

HTTP-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложения.

Сертификат Сервера администрирования

Сертификат, на основании которого осуществляется аутентификация Сервера администрирования при подключении к нему Консоли администрирования и обмене информацией с клиентскими устройствами. Сертификат Сервера администрирования создается при установке Сервера администрирования и хранится на Сервере администрирования в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

Состояние защиты

Текущее состояние защиты, характеризующее степень защищенности устройства.

Состояние защиты сети

Текущее состояние защиты, характеризующее степень защищенности устройств сети организации. Состояние защиты сети включает такие факторы, как наличие на устройствах сети установленных приложений защиты, использование ключей, количество и виды обнаруженных угроз.

Срок действия лицензии

Период времени, в течение которого вы можете пользоваться функциями приложения и дополнительными услугами. Объем доступных функций и дополнительных услуг зависит от типа лицензии.

Удаленная установка

Установка приложений "Лаборатории Касперского" при помощи инструментов, предоставляемых приложением Kaspersky Security Center Linux.

Управляемые устройства

Устройства сети организации, включенные в одну из групп администрирования.

Уровень важности патча

Характеристика патча. Для патчей сторонних производителей или Microsoft существует пять уровней важности:

- Предельный.
- Высокий.
- Средний.
- Низкий.
- Неизвестно.

Уровень важности патча стороннего производителя или Microsoft определяется наиболее неблагоприятным уровнем критичности уязвимости, которую закрывает патч.

Уровень важности события

Характеристика события, зафиксированного в работе приложения "Лаборатории Касперского". Существуют четыре уровня 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.

Уязвимость

Недостаток в операционной системе или приложении, который может быть использован злоумышленниками для проникновения в операционную систему или приложение и нарушения их целостности. Большое количество уязвимостей в операционной системе делает ее работу ненадежной, так как внедрившиеся в операционную систему вредоносные программы могут вызывать сбои в работе как самой операционной системы, так и установленных приложений.

Файл ключа

Файл вида xxxxxxxx.key, который позволяет использовать приложение "Лаборатории Касперского" по пробной или коммерческой лицензии. Вы можете использовать приложение только при наличии файла ключа.

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 приложением

Удаленное управление приложением при помощи сервисов 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 директории установки приложения.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe, Acrobat, Flash, PostScript, Shockwave 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 в Соединенных Штатах и/или других странах.

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 являются зарегистрированными товарными знаками или товарными знаками Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

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, США и/или 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 Famatech.

Firebird – зарегистрированный товарный знак Firebird Foundation.

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 являются товарными знаками 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 являются товарными знаками Mozilla Foundation 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.

OpenVPN – зарегистрированный товарный знак OpenVPN, Inc.

Oracle, Java, JavaScript, TouchDown – зарегистрированные товарные знаки компании Oracle и/или 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 Puppet, Inc.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

Red Hat, Fedora, Red Hat Enterprise Linux – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

Ansible является зарегистрированным товарным знаком Red Hat, Inc. в США и других странах.

CentOS – товарный знак или зарегистрированный в США и других странах товарный знак Red Hat, Inc. или дочерних компаний.

BlackBerry принадлежит Research In Motion Limited, зарегистрирован в США и может быть подан на регистрацию или зарегистрирован в других странах.

Rocky Linux является товарным знаком The Rocky Enterprise Software Foundation.

Samsung – товарный знак компании SAMSUNG в США или 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 компании The Linux Foundation.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

Zabbix – зарегистрированный товарный знак Zabbix SIA.