kaspersky

Kaspersky Security Center Cloud Console

© 2026 АО "Лаборатория Касперского"

Содержание

Справка Kaspersky Security Center Cloud Console

Что нового

Исправленные ошибки

Kaspersky Security Center Cloud Console

- Аппаратные и программные требования Kaspersky Security Center Cloud Console
- Совместимые приложения и решения "Лаборатории Касперского"
- Локализация приложения Kaspersky Security Center Cloud Console
- Сравнение Kaspersky Security Center и Kaspersky Security Center Cloud Console

Архитектура и основные понятия

- Архитектура
- Порты, используемые Kaspersky Security Center Cloud Console
- Основные понятия
  - Агент администрирования
  - Группы администрирования
  - Иерархия Серверов администрирования
  - Виртуальный Сервер администрирования
  - Точка распространения
  - Веб-плагин управления
  - Политики
  - Профили политик
  - Взаимосвязь политики и локальных параметров приложения

Лицензирование приложения

- Лицензирование приложения Kaspersky Security Center Cloud Console
- О пробной версии Kaspersky Security Center Cloud Console
- Использование Kaspersky Marketplace для выбора бизнес-решений
- Лицензии и минимальное количество устройств для каждой лицензии
- События превышения лицензионного ограничения
- Способы распространения кодов активации на управляемые устройства
- Добавление лицензионного ключа Сервера администрирования
- Добавление лицензионного ключа в хранилище Сервера администрирования
- Распространение лицензионного ключа на клиентские устройства
- Автоматическое распространение лицензионного ключа
- Просмотр информации об используемых лицензионных ключах в хранилище Сервера администрирования
- Просмотр информации о лицензионных ключах для выбранного приложения "Лаборатории Касперского"
- Удаление лицензионного ключа Сервера администрирования
- Удаление лицензионного ключа из хранилища
- Просмотр списка устройств, на которых приложение "Лаборатории Касперского" не активировано
- Отзыв согласия с Лицензионным соглашением
- Продление срока действия лицензии приложений "Лаборатории Касперского"
- Использование Kaspersky Security Center Cloud Console после истечения срока действия лицензии
- Определения лицензирования
  - О лицензии
  - О Лицензионном сертификате

- О лицензионном ключе
- О коде активации
- О подписке

Предоставление данных

- Данные, отправленные на серверы "Лаборатории Касперского"
- Данные, необходимые для работы управляемых приложений
- Данные Пользователя, обрабатываемые локально
- О юридических документах Kaspersky Security Center Cloud Console

Руководство по усилению защиты

- Планирование архитектуры Kaspersky Security Center Cloud Console
- Учетные записи и авторизация
- управление защитой клиентских устройств;
- Настройка защиты управляемых приложений
- Передача событий в сторонние системы
- Рекомендации по безопасности сторонних информационных систем
- Рекомендации по использованию приложений безопасности "Лаборатории Касперского"

Интерфейс Kaspersky Security Center Cloud Console

- Изменение языка интерфейса Kaspersky Security Center Cloud Console
- Изменение домашней страницы Kaspersky Security Center Cloud Console
- Закрепление и отмена закрепления разделов главного меню
- Возврат к списку рабочих областей

Первоначальная конфигурация Kaspersky Security Center Cloud Console

Сценарий: создание иерархии Серверов администрирования, управляемых с помощью Kaspersky Security Center Cloud Console

Перенос данных в Kaspersky Security Center Cloud Console

- Способы переноса данных в Kaspersky Security Center Cloud Console
- Сценарий: перенос данных без иерархии Серверов администрирования
- Мастер переноса данных
  - Шаг 1. Экспорт управляемых устройств, объектов и параметров из Kaspersky Security Center Web Console
  - Шаг 2. Импорт файла экспорта в Kaspersky Security Center Cloud Console
  - Шаг 3. Переустановка Агента администрирования на управляемых устройствах с помощью Kaspersky Security Center Cloud Console
- Перенос данных с иерархией Серверов администрирования
- Сценарий: перенос данных устройств с операционными системами Linux или macOS
- Сценарий: обратный перенос данных из Kaspersky Security Center Cloud Console в Kaspersky Security Center
- Перенос данных с виртуальными Серверами администрирования
  - Сценарий: перенос данных с виртуальными Серверами администрирования с помощью перемещения устройств
  - Сценарий: перенос данных с виртуальными Серверами администрирования вручную
  - Сценарий: перемещение устройств из групп администрирования под управление виртуальных Серверов

Мастер первоначальной настройки

- О мастере первоначальной настройки
- Запуск мастера первоначальной настройки
- Шаг 1. Выбор инсталляционных пакетов для загрузки
- Шаг 2. Настройка параметров прокси-сервера
- Шаг 3. Настройка Kaspersky Security Network
- Шаг 4. Настройка управления обновлениями приложений сторонних производителей

Шаг 5. Создание базовой конфигурации защиты сети
Шаг 6. Завершение работы мастера первоначальной настройки
Первоначальное развертывание приложений "Лаборатории Касперского"
Сценарий: первоначальное развертывание приложений "Лаборатории Касперского"
Создание инсталляционных пакетов для приложений "Лаборатории Касперского"
Распространение инсталляционных пакетов на подчиненные Серверы администрирования
Создание автономных инсталляционных пакетов Агента администрирования
Просмотр списка автономных инсталляционных пакетов
Создание пользовательского инсталляционного пакета
Требования для точки распространения
Параметры инсталляционного пакета Агента администрирования
Виртуальная инфраструктура
Рекомендации по снижению нагрузки на виртуальные машины
Поддержка динамических виртуальных машин
Поддержка копирования виртуальных машин
Использование Агента администрирования для Windows, Linux и macOS: сравнение
Указание параметров удаленной установки на устройствах под управлением Unix
Замещение приложений безопасности сторонних производителей
Возможности ручной установки приложений
Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center Cloud Console
Мастер развертывания защиты
Шаг 1. Запуск мастера развертывания защиты
Шаг 2. Выбор инсталляционного пакета
Шаг 3. Выбор версии Агента администрирования
Шаг 4. Выбор устройств
Шаг 5. Задание параметров задачи удаленной установки
Шаг 6. Управление перезагрузкой
Шаг 7. Удаление несовместимых приложений перед установкой
Шаг 8. Перемещение устройств в папку Управляемые устройства
Шаг 9. Выбор учетных записей для доступа к устройствам
Шаг 10. Запуск установки
Сетевые параметры для взаимодействия с внешними сервисами
Подготовка устройства под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования
Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux
Установка приложений с помощью задачи удаленной установки
Удаленная установка приложений
Установка приложений на подчиненные Серверы администрирования
Запуск и остановка приложений "Лаборатории Касперского"
Управление мобильными устройствами
Возможности обнаружения и реагирования
Data Discovery
О Data Discovery
Категории информации, обнаруживаемой Data Discovery

Начало использования Data Discovery
Принятие условий Соглашения о Data Discovery
Подключение организации Microsoft 365 к рабочей области
Просмотр информации об обнаружениях Data Discovery
Пример анализа обнаружения Data Discovery
Экспорт информации об обнаружениях Data Discovery
Выключение Data Discovery
Обнаружение сетевых устройств и создание групп администрирования
Сценарий: обнаружение сетевых устройств
Опрос сети
Опрос сети Windows
Опрос контроллеров домена
Опрос IP-диапазонов
Настройка контроллеров домена Samba
Добавление и изменение IP-диапазона
Настройка точек распространения и шлюзов соединений
Расчет количества и конфигурации точек распространения
Типовая конфигурация точек распространения: один офис
Типовая конфигурация точек распространения: множество небольших удаленных офисов
Назначение точек распространения вручную
Изменение списка точек распространения для группы администрирования
Использование точки распространения в качестве извещающего сервера
Использование параметра "Не разрывать соединение с Сервером администрирования" для обеспечения постоянной связи между управляемым устройством и Сервером администрирования
Создание групп администрирования
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
Настройка правил хранения для нераспределенных устройств
Инвентаризация оборудования
Добавление информации о новых устройствах
Настройка критериев определения корпоративных устройств
Настройка защиты сети
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
Параметры политики Агента администрирования
Сравнение параметров политики Агента администрирования по операционным системам
Настройка параметров защиты управляемых приложений
Ручная настройка групповой задачи обновления Kaspersky Endpoint Security
Задачи
О задачах
Область задачи
Создание задачи

Просмотр списка задач
Запуск задачи вручную
Запуск задачи для выбранных устройств.
Общие параметры и свойства задач
Экспорт задачи
Импорт задачи
Просмотр результатов выполнения задач, хранящихся на Сервере администрирования
Управление клиентскими устройствами
Параметры управляемого устройства
Проверка соединения клиентского устройства с Сервером администрирования вручную Утилита klnagchk
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
Просмотр и настройка действий, когда устройство неактивно
О статусах устройства
Настройка переключения статусов устройств
Смена Сервера администрирования для клиентских устройств
Избегание конфликтов между Серверами администрирования
Создание профилей подключения к Серверу администрирования
О кластерах и массивах серверов
Свойства кластеров или массивов серверов
Теги устройств
Создание тегов устройств
Изменение тегов устройств
Удаление тегов устройств
Просмотр устройств, которым назначен тег
Просмотр тегов, назначенных устройству
Назначение тегов устройствам вручную
Снятие назначенных тегов с устройств
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
Карантин и Файлы резервного хранилища
Загрузка файла из хранилища
Удаление файлов из хранилища
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 приложения и загрузка результатов
Запуск приложения на клиентском устройстве
Создание файла дампа для приложения
Удаленное подключение к рабочему столу клиентского устройства
Подключение к устройствам с помощью совместного доступа к рабочему столу Windows
Срабатывание правил в режиме Интеллектуального обучения
Просмотр списка обнаружений, выполненных с помощью правил Адаптивного контроля аномалий
Добавление исключений в правила Адаптивного контроля аномалий
Управление группами администрирования
Создание групп администрирования
Автоматическая установка приложений на устройства группы администрирования
Перемещение групп администрирования
Удаление групп администрирования
Политики и профили 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
Изменение политики
Общие параметры политик
Включение и выключение параметра наследования политики
Копирование политики
Перемещение политики
Экспорт политики
Импорт политики
Просмотр диаграммы состояния применения политики
Автоматическая активация политики по событию "Вирусная атака"
Принудительная синхронизация
Удаление политики
Управление профилями политик
Просмотр профилей политики
Изменение приоритета профиля политики
Создание профиля политики
Изменение профиля политики
Копирование профиля политики
Создание правила активации профиля политики
Удаление профиля политики
Экспорт и импорт профиля политики

Шифрование и защита данных
Просмотр списка зашифрованных жестких дисков
Формирование и просмотр отчетов о шифровании
Предоставление доступа к зашифрованному жесткому диску в автономном режиме
Пользователи и роли пользователей
Об учетных записях пользователей
Добавление учетной записи внутреннего пользователя
Удаление учетной записи внутреннего пользователя
Назначение администраторов рабочей области
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
Назначение роли пользователю или группе безопасности
Создание роли пользователя
Изменение роли пользователя
Изменение области для роли пользователя
Удаление роли пользователя
Связь профилей политики с ролями
Создание группы безопасности
Изменение группы безопасности
Добавление учетных записей пользователей во внутреннюю группу
Удаление группы безопасности
Настройка ADFS-интеграции
Настройка интеграции с Microsoft Entra ID
Включение опроса Microsoft Entra ID
Добавление Kaspersky Security Center Cloud Console в список приложений
Назначение пользователя владельцем устройства
Назначение пользователя владельцем устройства Linux после установки Агента администрирования
Работа с ревизиями объектов
Добавление описания ревизии
Откат изменений объекта к предыдущей ревизии
Просмотр и сохранение ревизии политики
Сравнение ревизий политики
Kaspersky Security Network (KSN)
О KSN
Включение и отключение KSN
Просмотр принятого Положения о KSN
Принятие обновленного Положения о KSN
Проверка, работает ли точка распространения как прокси-сервер KSN
Удаление объектов
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 загрузки обновлений в хранилища точек распространения

Настройка управляемых устройств для получения обновлений только от точек распространения
Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center Cloud Console
Автоматическая установка обновлений для Kaspersky Endpoint Security для Windows
О статусах обновлений
Одобрение и отклонение обновлений программного обеспечения
Использование файлов различий для обновления баз и модулей приложений "Лаборатории Касперского".
Обновление баз и модулей приложений "Лаборатории Касперского" на автономных устройствах
Управление приложениями сторонних производителей на клиентских устройствах
Ограничения Системного администрирования
Доступность Системного администрирования в пробном и коммерческом режимах и при различных вариантах лицензирования
О приложениях сторонних производителей
Обновления приложений сторонних производителей
Сценарий: обновление приложений сторонних производителей
Установка обновлений приложений сторонних производителей
Создание задачи Поиск уязвимостей и требуемых обновлений
Параметры задачи поиска уязвимостей и требуемых обновлений
Создание задачи Установка требуемых обновлений и закрытие уязвимостей
Добавление правил для установки обновлений
Создание задачи Установка обновлений Центра обновления Windows
Просмотр информации о доступных обновлениях приложений сторонних производителей.
Экспорт списка доступных обновлений в файл
Одобрение и отклонение обновлений приложений сторонних производителей.
Автоматическое обновление приложений сторонних производителей
Обнаружение и закрытие уязвимостей в приложениях
Закрытие уязвимостей в приложениях
Создание задачи Закрытие уязвимостей
Создание задачи Установка требуемых обновлений и закрытие уязвимостей
Добавление правил для установки обновлений
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
Сценарий: обнаружение и закрытие уязвимостей в приложениях
Установка максимального срока хранения информации о закрытых уязвимостях
Управление запуском приложений на клиентских устройствах
Использование компонента Контроль приложений для управления исполняемыми файлами
Режимы и категории компонента Контроль приложений
Получение и просмотр списка приложений, установленных на клиентских устройствах
Получение и просмотр списка исполняемых файлов, установленных на клиентских устройствах
Создание пополняемой вручную категории приложений
Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств
Просмотр списка категорий приложений
Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows
Добавление исполняемых файлов, связанных с событием, в категорию приложения

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"
Теги приложений
Создание тегов приложений
Изменение тегов приложений
Назначение тегов приложениям
Снятие назначенных тегов с приложений
Удаление тегов приложений
Настройка Сервера администрирования
Иерархия Серверов администрирования
Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования
Настройка срока хранения событий, относящихся к удаленным устройствам
Объединение электронной почты о событиях
Ограничения на управление подчиненными Серверами администрирования, работающими локально, с помощью Kaspersky Security Center Cloud Console
Просмотр списка подчиненных Серверов администрирования
Удаление иерархии Серверов администрирования
Настройка интерфейса
Управление виртуальными Серверами администрирования
Создание виртуального Сервера администрирования
Включение и выключение виртуального Сервера администрирования
Назначение администратора виртуального Сервера администрирования
Удаление виртуального Сервера администрирования
Мониторинг и отчеты
Сценарий: мониторинг и отчеты
О типах мониторинга и отчетах
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

- События и выборки событий
  - О событиях в Kaspersky Security Center Cloud Console
  - События компонентов Kaspersky Security Center Cloud Console
    - 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
  - Хранение информации о событиях для задач и политик
  - Удаление событий
  - Удаление выборок событий
  - Блокировка частых событий
    - О блокировке частых событий
    - Управление блокировкой частых событий
    - Отмена блокировки частых событий
- Уведомления и статусы устройств
  - Об уведомлениях
  - Просмотр уведомлений, требующих внимания
  - Просмотр системных уведомлений
  - Просмотр объявлений
  - Выключение объявлений
  - Настройка переключения статусов устройств
  - Настройка параметров доставки уведомлений
- Получение предупреждения об истечении срока лицензии
- 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

Активные угрозы
Дезинфекция необработанного файла
Скачивание необработанного файла
Удаление файлов из раздела Активные угрозы
Использование Kaspersky Security Center Cloud Console 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
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 приложения и загрузка результатов
Запуск приложения на клиентском устройстве
Создание файла дампа для приложения
Запуск удаленной диагностики на клиентском устройстве с операционной системой Linux
Экспорт событий в SIEM-системы
Настройка экспорта событий в SIEM-системы
Предварительные условия
Об экспорте событий
Настройка экспорта событий в SIEM-системе
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 Cloud Console для экспорта событий в SIEM-систему
Просмотр результатов экспорта
Руководство по первоначальной настройке для поставщиков управляемых услуг (MSP)
О Kaspersky Security Center Cloud Console
Основные функции Kaspersky Security Center Cloud Console
О лицензировании Kaspersky Security Center Cloud Console для поставщиков услуг
О возможностях обнаружения и реагирования для поставщиков услуг
Начало работы с Kaspersky Security Center Cloud Console
Рекомендации по управлению устройствами ваших клиентов
Типовые способы развертывания системы защиты для поставщиков услуг
Сценарий: развертывание защиты (управление тенантами с помощью виртуальных Серверов администрирования)
Сценарий: развертывание защиты (управление с помощью групп администрирования)
Совместное использование приложения Kaspersky Security Center, работающего локально, и Kaspersky Security Center Cloud Console

Лицензирование приложений "Лаборатории Касперского" для поставщиков услуг
Функции мониторинга и работа с отчетами для поставщиков услуг
Работа с Kaspersky Security Center Cloud Console в облачном окружении
Варианты лицензирования в облачном окружении
Подготовка к работе в облачном окружении с помощью Kaspersky Security Center Cloud Console
Работа в облачном окружении Amazon Web Services
О работе в облачном окружении Amazon Web Services
Создание учетных записей IAM-пользователя для инстансов Amazon EC2
Обеспечение прав для работы Kaspersky Security Center Cloud Console с AWS
Создание учетной записи IAM-пользователя для работы Kaspersky Security Center Cloud Console
Работа в облачном окружении Microsoft Azure
О работе в Microsoft Azure
Создание подписки, идентификатора приложения и пароля
Назначение роли для ID приложения в Azure
Работа в Google Cloud
Мастер настройки для работы в облачном окружении в Kaspersky Security Center Cloud Console
Шаг 1. Проверка требуемых плагинов и инсталляционных пакетов
Шаг 2. Выбор способа активации приложения
Шаг 3. Выбор облачного окружения и аутентификация
Шаг 4. Опрос сегментов и настройка синхронизации с облачным окружением
Шаг 5. Настройка Kaspersky Security Network для Kaspersky Security Center Cloud Console
Шаг 6. Создание первоначальной конфигурации защиты
Опрос сегмента сети с помощью Kaspersky Security Center Cloud Console
Добавление подключений для опроса облачных сегментов через Kaspersky Security Center Cloud Console
Удаление соединения для опроса облачных сегментов
Настройка расписания опроса с помощью Kaspersky Security Center Cloud Console
Просмотр результатов опроса облачного сегмента с помощью Kaspersky Security Center Cloud Console
Просмотр свойств облачных устройств с помощью Kaspersky Security Center Cloud Console
Синхронизация с облачным сегментом: настройка правила перемещения
Удаленная установка приложений на виртуальные машины Azure
Руководство по масштабированию
Об этом руководстве
Лучшие практики для Сервера администрирования, управляющего большим количеством устройств
Обращение в Службу технической поддержки
Способы получения технической поддержки
Техническая поддержка через Kaspersky CompanyAccount
Информация, необходимая специалистам Службы технической поддержки "Лаборатории Касперского"
Источники информации о приложении
Известные проблемы и ограничения
Глоссарий
AWS Application Program Interface (AWS API)
Cloud discovery
HTTPS
IAM-пользователь
IAM-роль
Identity and Access Management (IAM)
JavaScript

Kaspersky Security Center Cloud Console

Kaspersky Security Network (KSN)

Lightweight Nagent (LWNGT)

Network Location Awareness (NLA)

Push-сервер

SSL

Агент администрирования

Агент аутентификации

Агент обновлений

Администратор Kaspersky Security Center Cloud Console

Активный ключ

Антивирусная безопасность сети

Антивирусные базы

Веб-плагин управления

Виртуальный Сервер администрирования

Вирусная атака

Владелец устройства

Восстановление

Группа администрирования

Групповая задача

Демилитаризованная зона (DMZ)

Домашний Сервер администрирования

Дополнительный ключ

Доступное обновление

Задача

Задача для набора устройств

Инсталляционный пакет

Инстанс Amazon EC2

Карантин

Ключ доступа IAM AWS

Консоль AWS

Локальная задача

Локальная установка

Настройки задачи

Непосредственное управление приложением

Несовместимое приложение

Обновление

Образ AMI

Оператор Kaspersky Security Center Cloud Console

Параметры приложения

Политика

Порог вирусной активности

Профиль политики

Рабочая область

Сервер администрирования

Серверы обновлений "Лаборатории Касперского"

Состояние защиты

Состояние защиты сети
Срок действия лицензии
Тег приложения
Тег устройства
Удаленная установка
Управляемое устройство
Уровень важности патча
Уровень важности события
Устройство с защитой на уровне UEFI
Учетная запись Kaspersky Security Center Cloud Console
Уязвимость
Файл ключа
Форсированная установка
Хранилище событий
Централизованное управление приложением
Широковещательный домен
Шлюз соединения
Информация о стороннем коде
Trademark notices

Справка Kaspersky Security Center Cloud Console

	**Что нового** Узнайте, что нового в этой версии приложения.		**Настройка защиты сети** Управляйте безопасностью организации, настраивая политики и задачи "Лаборатории Касперского" в соответствии с требованиями организации.
	**Аппаратные и программные требования** Проверьте поддерживаемые операционные системы и версии приложений.		**Приложения "Лаборатории Касперского": регулярное обновление баз и модулей приложений** Поддержка надежности системы защиты.
	**Лицензирование приложения Kaspersky Security Center Cloud Console** Узнайте подробнее о пробной версии и коммерческой версии приложения Kaspersky Security Center Cloud Console.		**Мониторинг и отчеты** Просматривайте данные об инфраструктуре вашей сети и статусе защиты сетевых устройств, а также статистику, чтобы управлять текущим состоянием защиты вашей организации. Вы также можете использовать отчеты.
	**Первоначальная настройка** Начните работать с вашей рабочей областью, настройте Kaspersky Security Center Cloud Console в соответствии с вашими требованиями.		**Системное администрирование.** Обнаружение и закрытие уязвимостей в приложениях сторонних производителей.
	**Перенос данных в Kaspersky Security Center Cloud Console** Перенос данных существующих групп администрирования и связанных с ними объектов из локального Kaspersky Security Center в Kaspersky Security Center Cloud Console.		**Экспорт событий в SIEM-системы** Настройте экспорт событий в SIEM-системы с помощью формата Syslog.
	**Обнаружение устройств в сети** Обнаружение существующих и новых устройств в сети вашей организации.		**Работа в облачном окружении** Защита виртуальных машин в облачных окружениях: Amazon Web Services™, Microsoft Azure™, Google™ платформа Google Cloud.
	**Расчеты для точек распространения и/или шлюзов соединений** Настройка точек распространения.		**Использование функциональности Kaspersky Security для бизнеса Профессиональный в Kaspersky Security Center Cloud Console** Настройте интеграцию для реагирования на алерты и агрегирования алертов, относящихся к одному инциденту, чтобы упростить процесс расследования.
	**Приложения "Лаборатории Касперского": первоначальное развертывание** Развертывание приложений "Лаборатории Касперского".		**Руководство по первоначальной настройке для поставщиков управляемых услуг (MSP)** Узнайте, как работать с Kaspersky Security Center Cloud Console, если вы являетесь администратором поставщика услуг.

Что нового

Обновление от августа 2026

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие улучшения:

- Теперь доступен Центр уведомлений. Центр уведомлений отображает уведомления и объявления, которые помогают вам быть в курсе соответствующих событий, изменений и рекомендаций, связанных с вашим Сервером администрирования и управляемыми устройствами. Вы можете искать, сортировать и фильтровать уведомления в таблице. Все непрочитанные уведомления также доступны при нажатии на значок уведомления ( ) рядом с меню вашей учетной записи.
- Изменено окно **Новый пользовательский инсталляционный пакет**. Окно теперь включает средство загрузки файлов, и когда размер инсталляционного пакета для выборочной установки превышает ограничение, приложение отображает сообщение об ошибке.
- Kaspersky Security Center Cloud Console теперь поддерживает работу с:
  - Kaspersky Endpoint Security 14.1 для Windows.
  - Kaspersky Endpoint Security 12.5 для Linux.

Обновление от июня 2026

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие улучшения:

- Теперь вы можете назначать администраторов сразу нескольким виртуальным Серверам.
- Теперь вы можете переключать рабочие области из пробного режима в коммерческий режим. После перехода рабочая область не будет удалена по истечении 30-дневного периода.
- Теперь вы можете добавлять новых пользователей в свою рабочую область в разделе Пользователи и роли. Вы также можете назначить новых пользователей администраторами рабочей области.
- Добавлен список данных, обрабатываемых Kaspersky при подключении устройств.

- Повышено удобство работы с приложением:
  - Улучшен процесс назначения точек распространения: в списке теперь отображаются только неназначенные точки распространения.
  - Улучшен алгоритм обнаружения сетевых устройств. 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.
  - Улучшен раздел **Навигация консоли** для более эффективного использования пространства экрана.
  - Повышено удобство восприятия информации отображаемых уведомлений в различных сценариях работы системы.
- Kaspersky Security Center Cloud Console поддерживает работу с:
  - Kaspersky Endpoint Security 14.0 для Windows.
  - Kaspersky Embedded Systems Security 4.0 для Linux.
  - Data Discovery: обнаружение большего количества типов конфиденциальных данных и предотвращение утечки критически важной или персональной информации.
  - iOS MDM Server: подключение мобильных устройств iOS к Серверу администрирования и управление ими с помощью службы Apple Push Notification (APNs).

Обновление от февраля 2026

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие улучшения:

- 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 Cloud Console: число элементов на страницу по умолчанию увеличено до 50, а настроенное число элементов теперь сохраняется от сеанса к сеансу.
- Kaspersky Security Center Cloud Console теперь поддерживает работу со следующими приложениями "Лаборатории Касперского":
  - Kaspersky Endpoint Security 12.12 для Windows.
  - Kaspersky Endpoint Security 12.4 для Linux.

- Агент администрирования теперь поддерживает работу со следующими новыми версиями операционных систем:
  - CentOS Stream 10 64-разрядная.
  - Debian GNU/Linux 13 (Trixie) 64-разрядная.
  - Red Hat Enterprise Linux Server 10.x 64-разрядная.
- Инфраструктура Kaspersky Security Center Cloud Console теперь поддерживает лицензии Kaspersky Next XDR Ultimate.
- Вы можете пройти обучение по кибербезопасности, позволяющее стать профессионалами в сфере ИТ-безопасности.

Обновление от октября 2025

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие улучшения:

- Поддерживаются контроллеры домена FreeIPA и ALD Pro.
- 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 **Активы (Устройства)**.
    - Раздел **Быстрые ссылки** теперь называется **Навигация консоли**.
  - При необходимости вы можете свернуть главное меню до значков.
- 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 Cloud Console теперь поддерживает работу с:
  - Microsoft Windows 11 25H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная.
  - Со следующими приложениями "Лаборатории Касперского":
    - Kaspersky Endpoint Security 12.11 для Windows.
    - Kaspersky Embedded Systems Security 4.0 для Windows.

Обновление от сентября 2025

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие улучшения:

- 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.
- Мы больше не используем понятие "компании", только "рабочие области". Поэтому существующие рабочие области были переименованы в следующем формате: `[<название компании>]<название рабочей области>`.
- В инфраструктуре Kaspersky Security Center Cloud Console появилась отдельная вкладка **Лицензии**. Если одна лицензия используется для нескольких рабочих областей, на вкладке **Лицензии** можно просмотреть суммарное использование этой лицензии.
- На новой вкладке **Лицензии** вы также можете просмотреть актуальные юридические документы для программных решений и приложений безопасности, доступных в Kaspersky Security Center Cloud Console.
- С помощью специальных виджетов и баннеров в инфраструктуре Kaspersky Security Center Cloud Console администраторы поставщиков управляемых услуг (MSP) теперь смогут следить за основными показателями работы во всех своих рабочих областях.

Обновление от июля 2025

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие улучшения:

- 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.
- Некоторые версии Агента администрирования не поддерживаются. Ознакомьтесь со страницей жизненного цикла поддержки приложений и при необходимости обновите Агент администрирования до актуальной версии **со статусом Полная поддержка** или **Ограниченная поддержка**.
- Кнопка **Проверка** удалена из раздела **Карантин**.

- Kaspersky Security Center Cloud Console теперь поддерживает следующие приложения "Лаборатории Касперского":
  - Kaspersky Endpoint Security 12.10 для Windows.
  - Kaspersky Endpoint Security 12.3 для Linux.
  - Kaspersky Endpoint Security 12.2 для Mac.
- Улучшен пользовательский интерфейс для создания рабочей области и управления ею.

Обновление от апреля 2025

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие улучшения:

- Kaspersky Security Center Cloud Console теперь поддерживает следующие приложения "Лаборатории Касперского":
  - Kaspersky Embedded Systems Security 3.4 для Linux.
  - Kaspersky Endpoint Security 12.2 для Linux.
  - Kaspersky Endpoint Security 12.8 для Windows.
- Загрузите и запустите приложение (или скрипт) для диагностики на управляемом устройстве. Теперь вы можете загрузить либо папку или архив, содержащий исполняемый файл, либо сам исполняемый файл. После успешного выполнения приложения, вы можете скачать результаты выполнения.
- Информация о пользователях, в настоящее время вошедших в систему на управляемом устройстве Linux, теперь отображается в окне свойств устройства в разделе **Общие → Сеансы**.
- Поддержка новых языков: инфраструктура Kaspersky Security Center Cloud Console доступна на китайском упрощенном языке.
- Улучшен пользовательский опыт:
  - Доступные инсталляционные пакеты отображаются на одной вкладке.
  - Вы можете изменить параметры домашней страницы с помощью нового раздела **Быстрые ссылки**. По умолчанию вкладка **Параметры домашней страницы** раздела **Быстрые ссылки** установлена как домашняя страница.
  - Обновлена навигация по группам администрирования: перейти в нужную подгруппу можно, нажав на ссылку с ее названием в пути к группе администрирования.
  - Раздел главного меню **Закрепленное** теперь называется **Закладки**. Вы можете добавить разделы Kaspersky Security Center Cloud Console в закладки, чтобы быстро получать к ним доступ.

Обновление от февраля 2025

Это обновление Kaspersky Security Center Cloud Console повышает производительность при открытии и навигации по Web Console.

Обновление от октября 2024

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие улучшения:

- Улучшена интеграция с Microsoft Entra ID. Теперь, когда пользователь выходит из учетной записи Microsoft Entra ID, которая использовалась для аутентификации в Kaspersky Security Center Cloud Console, сеанс также завершается для Kaspersky Security Center Cloud Console и пользователь автоматически выходит из консоли.
- Теперь вы можете просматривать и скачивать ревизии политики. Kaspersky Security Center Cloud Console позволяет просматривать отчет в формате HTML или сохранять ревизию в файл JSON.
- Теперь Kaspersky Security Center Cloud Console отображает последний статус задачи, известный Серверу администрирования.
- **Отчет о сетевых атаках** теперь включает MAC-адрес и порт атакующей машины.
- Теперь вы можете закрыть правую панель, нажав на кнопку мыши в любом месте за пределами панели. Если вы внесете какие-либо изменения в панель и затем попытаетесь закрыть ее, нажав на кнопку мыши за пределами панели, появится окно подтверждения.
- Заголовок таблицы теперь остается закрепленным в верхней части при прокрутке таблицы.

Обновление от сентября 2024

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие улучшения:

- Поддерживается Kaspersky Endpoint Agent 4.0.
- Больше не поддерживаются устаревшие браузеры (версии Chrome ниже чем 128, версии Edge ниже чем 128, версии Firefox ESR ниже чем 115, версии Safari ниже чем 17.6).

Обновление от апреля 2024

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие новые функции и улучшения:

- Новая функция Cloud Discovery. Эта функция позволяет контролировать использование облачных сервисов на управляемых устройствах с операционной системой Windows и блокировать доступ к облачным сервисам, которые вы считаете нежелательными. Cloud Discovery отслеживает попытки пользователей получить доступ к этим службам через браузеры и настольные приложения.

- Интеграция с Microsoft Entra ID позволяет пользователям вашей организации входить в Kaspersky Security Center Cloud Console под учетными данными Microsoft Entra ID. Обратите внимание, эта функция недоступна в Российской Федерации.

- Теперь вы можете создавать профили соединения для подключения Агента администрирования к Серверу администрирования. Профили соединения позволяют автономным пользователям, использующим ноутбуки, изменить способ подключения к Серверу администрирования или переключиться между Серверами администрирования в зависимости от текущего расположения устройства в сети.

- Теперь вы можете открыть список своих рабочих областей напрямую из главного меню приложения.

- Были добавлены два новых языка локализации – традиционный китайский и упрощенный китайский.

- Параметр хранения событий по умолчанию в свойствах задачи изменен с **Сохранять все события** на **Сохранять только результат выполнения задачи**. Этот параметр уменьшает использование места в базе данных рабочей области. Изменение касается только задач, созданных для Kaspersky Security Center. Этот параметр остается неизменным в задачах для приложений безопасности "Лаборатории Касперского".

- Kaspersky Security Center Cloud Console теперь дополнительно уведомляет вас о планируемом удалении вашей рабочей области через 7 и 30 дней после удаления или истечения срока действия последнего лицензионного ключа. Это даст вам больше времени, чтобы приобрести другую лицензию и добавить лицензионный ключ в рабочую область.

- Инфраструктура Kaspersky Business Hub и Kaspersky Security Center Cloud Console теперь поддерживает лицензии Kaspersky. Логотип приложения изменяется автоматически в соответствии с используемой вами лицензией.

- Kaspersky Security Center Cloud Console теперь поддерживает следующие приложения "Лаборатории Касперского":
  - Kaspersky Endpoint Security для Windows версия 12.4.
  - Kaspersky Endpoint Security 12.0 для Mac патч A.

- Если вы переносите данные из одного приложения безопасности "Лаборатории Касперского" в другое и текущее приложение защищено паролем, вы можете указать пароль для удаления напрямую в свойствах задачи удаленной установки.

- Теперь вы можете настроить главное меню приложения, закрепив или отменив закрепление избранных разделов меню. Закрепленные разделы добавляются в область **Закрепленные** для быстрого доступа.

- Оптимизирован интерфейс приложения и взаимодействие с пользователем при выборе параметра **По завершении другой задачи** при планировании задачи.
- Отчет об оборудовании теперь может включать информацию об устройствах macOS.
- Теперь вы можете выбрать одно или несколько клиентских устройств в списке устройств и запустить для них ранее созданную задачу.

Обновление от февраля 2024

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие новые функции и улучшения:

- В списке управляемых устройств теперь можно выбрать устройство или несколько устройств и назначить им существующую задачу для запуска. Текущая область действия задачи будет заменена выбранными вами устройствами.
- Теперь вы можете назначать теги нескольким устройствам или удалять теги с нескольких устройств сразу. В списке управляемых устройств выберите устройства и укажите, какие теги вы хотите назначить или удалить с выбранных устройств.
- Оптимизирован внешний вид и удобство использования списка управляемых устройств. Добавлен столбец **Теги** и возможность фильтровать устройства по тегам устройств.

Обновление от января 2024

Kaspersky Security Center Cloud Console поддерживает Kaspersky Endpoint Security 12.4 для Windows.

Обновление от декабря 2023 года

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие новые функции и улучшения:

- Теперь вы можете проверить подключение к SIEM-системе.
- Kaspersky Security Center Cloud Console теперь поддерживает опрос контроллеров домена Microsoft Active Directory и контроллеров домена Samba с помощью точки распространения с операционной системой Linux.
- Удаленная диагностика управляемых устройств с операционной системой Linux.

- Kaspersky Security Center Cloud Console теперь поддерживает следующие приложения "Лаборатории Касперского":
  - Kaspersky Endpoint Security для Windows версии 12.3 патч A.
  - Kaspersky Endpoint Security 12.0 для Linux.
  - Kaspersky Endpoint Security 12.0 для Mac.
  - Kaspersky Endpoint Agent 3.16.
  - Kaspersky Embedded Systems Security 3.3 для Windows.
- Из главного меню были скрыты два раздела интерфейса, выходящие за рамки функциональности приложения:
  - События шифрования (**Операции** → **Шифрование и защита данных** → **События шифрования**).
  - IP-диапазоны (**Обнаружение устройств и развертывание** → **Обнаружение устройств** → **IP-диапазоны**).
- Обновлен текст Соглашения об обработке данных для Kaspersky Security Center Cloud Console.
- Некоторые старые версии браузеров больше не поддерживаются (Firefox ESR версии ниже 102).

Обновление от сентября 2023

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие новые функции и улучшения:

- Kaspersky Security Center Cloud Console поддерживает Kaspersky Embedded Systems Security 3.3 для Linux.
- Kaspersky Security Center Cloud Console поддерживает Kaspersky Endpoint Security 12.2 для Windows.
- Оптимизирован пользовательский интерфейс при работе со списком пользователей в разделе **Управление активами**.

Обновление от июня 2023

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие новые функции и улучшения:

- Выпущено Руководство по усилению защиты. Настоятельно рекомендуется внимательно прочитать руководство и следовать рекомендациям по безопасности при настройке Kaspersky Security Center Cloud Console и вашей сетевой инфраструктуры.
- Kaspersky Security Center Cloud Console поддерживает Kaspersky Endpoint Security 11.3 для Mac.

- Kaspersky Security Center Cloud Console поддерживает Kaspersky Endpoint Security 11.4 для Linux.
- Вы можете использовать Kaspersky Security Center Cloud Console для экспорта выборок событий в файл и импорта выборок событий в Kaspersky Security Center Windows или Kaspersky Security Center Linux.
- Теперь вы можете использовать точку распространения в качестве push-сервера для устройств, управляемых Агентом администрирования. Эта функция позволяет установить постоянное соединение между управляемым устройством и Сервером администрирования.
- Реорганизован раздел с параметрами для интеграции Kaspersky Security Center Cloud Console с другими приложениями "Лаборатории Касперского".
- Реорганизован пользовательский интерфейс раздела **Удаленная диагностика**.
- Теперь можно сохранить информацию сразу обо всех устройствах, включенных в выборку устройств, в файл CSV.
- Улучшен пользовательский интерфейс, и повышено удобство работы с приложением, в том числе добавлена возможность выбора всех элементов в таблице.

Обновление от марта 2023

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие новые функции и улучшения:

- Kaspersky Security Center Cloud Console теперь поддерживает кластеры и массивы серверов в качестве управляемых устройств. Если приложение "Лаборатории Касперского" установлено на узле кластера, Агент администрирования отправляет эту информацию на Сервер администрирования. В Web Console кластеры и массивы серверов перечислены отдельно от других управляемых устройств. Вы управляете каждым кластером или массивом серверов как отдельным неделимым объектом.
- Kaspersky Security Center Cloud Console поддерживает Kaspersky Endpoint Security 12.0 для Windows.
- Максимальное количество записей, которое может быть включено в отчет было увеличено до 2500 для отчета в Web Console и до 10 000 для отчета, который вы экспортируете в файл.
- Теперь вы можете выбрать, включать управляемые устройства со статусом *OK* в отчет о состоянии защиты или нет.
- Теперь вы можете активировать Kaspersky Security Center Cloud Console с помощью одной из следующих лицензий или добавить перечисленные лицензионные ключи в существующую рабочую область:
  - Kaspersky Symphony Security
  - Kaspersky Symphony EDR
  - Kaspersky Symphony MDR
  - Kaspersky Symphony XDR
- Выпущена специальная редакция Агента администрирования для Windows XP.

- Обновленный Агент администрирования для Linux поддерживает службу прокси-сервера KSN. Наряду с точками распространения с операционной системой Windows теперь вы можете использовать точки распространения с операционной системой Linux для перенаправления запросов Kaspersky Security Network (KSN) от управляемых устройств. Эта функция позволяет перераспределить и оптимизировать трафик сети.

- Обновленный Агент администрирования для Linux поддерживает функциональность Реестр приложений. Агент администрирования может составить список приложений, установленных на устройстве с операционной системой Linux, и передать этот список Серверу администрирования.

- Вы можете использовать Kaspersky Security Center Cloud Console для экспорта политик и задач в файл, а затем импортировать политики и задачи в Kaspersky Security Center Windows или Kaspersky Security Center Linux.

Обновление от ноября 2022

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие новые функции и улучшения:

- Kaspersky Security Center Cloud Console поддерживает Kaspersky Endpoint Security 11.3 для Linux.

- Kaspersky Security Center Cloud Console теперь поддерживает Kaspersky Managed Detection and Response 2.1.18.

- Kaspersky Security Center Cloud Console теперь поддерживает обновленные версии Kaspersky Endpoint Security для Mac 11.2 и 11.2.1 для macOS 13.

- Обновлены видео в разделе **Обучающие материалы**.

Обновление от октября 2022

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие новые функции и улучшения:

- Обновлен текст Соглашения об обработке данных для Kaspersky Security Center Cloud Console.

- Инфраструктура Kaspersky Security Center Cloud Console теперь уведомляет вас о рабочей области, в которой нет активного лицензионного ключа и которая может быть удалена, если вы не добавите лицензионный ключ.

- Kaspersky Security Center Cloud Console поддерживает Kaspersky Endpoint Security 11.11.0 для Windows.

- Kaspersky Security Center Cloud Console теперь поддерживает Kaspersky Endpoint Detection and Response Optimum 2.3.

- Поддерживается Kaspersky Embedded Systems Security 3.2.

Обновление от сентября 2022

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие новые функции и улучшения:

- Теперь вы можете назначать выделенных администраторов для виртуальных Серверов администрирования. Вы создаете учетную запись для администратора, а затем предоставляете администратору права доступа к виртуальному Серверу администрирования. Назначенный администратор имеет доступ только к выбранному виртуальному Серверу администрирования и не может подключаться к главному Серверу администрирования или другим подчиненным Серверам администрирования, физическим или виртуальным.

- Оптимизирован интерфейс при удалении лицензионного ключа Kaspersky Security Center Cloud Console. Новый механизм предотвращает случайное удаление последнего активного лицензионного ключа.

- Теперь вы можете использовать точки распространения с операционной системой Linux для загрузки антивирусных баз для приложений безопасности "Лаборатории Касперского" с помощью задачи *Загрузка обновлений в хранилища точек распространения*.

- Агент администрирования доступен на японском языке.

- В интерфейсе Kaspersky Security Center Cloud Console изменен стиль названий разделов.

Обновление от августа 2022

Поддержка новых языков: Приложение Kaspersky Security Center Cloud Console доступна на японском языке.

Обновление от июля 2022

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие новые функции и улучшения:

- Новые версии поддерживаемых приложений "Лаборатории Касперского":
  - Kaspersky Endpoint Agent 3.13
  - Kaspersky Endpoint Security 11.2.1 для Mac
  - Kaspersky Security для iOS 1.0.0
  - Kaspersky Endpoint Security 11.10.0 для Windows

- Обновлен текст Лицензионного соглашения и Соглашения об обработке данных для Kaspersky Security Center Cloud Console.
- Поддержка новых языков: Инфраструктура Kaspersky Security Center Cloud Console теперь доступна на японском языке. Поддержка японского языка в рабочих областях Kaspersky Security Center Cloud Console появится в ближайшее время.

Обновление от апреля 2022

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие новые функции и улучшения:

- Kaspersky Security Center Cloud Console поддерживает Kaspersky Endpoint Security 11.9.0 для Windows.
- Kaspersky Security Center Cloud Console поддерживает японский язык для Kaspersky Embedded Systems Security.

Обновление от 9 марта 2022

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие новые функции и улучшения:

- Реализована интеграция с Kaspersky Endpoint Detection and Response Expert.
- Реализована платформа Incident Response Platform (IRP). Теперь можно управлять инцидентами безопасности с помощью Kaspersky Security Center Cloud Console.
- Kaspersky Security Center Cloud Console теперь использует лицензионные ключи для Kaspersky Endpoint Detection and Response Expert. Минимальное количество устройств для лицензии – 50.

Обновление от 11 февраля 2022

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие новые функции и улучшения:

- Теперь поддерживаются лицензии Kaspersky Embedded Systems Security для Windows.
- Поддерживается Kaspersky Endpoint Security 11.8.0 для Windows.
- Вы можете установить Kaspersky Endpoint Security 11.8.0 для Windows с помощью дистрибутива на японском языке.
- Поддерживается Kaspersky Endpoint Agent 3.12.

Обновление от 10 декабря 2021

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие новые функции и улучшения:

- Улучшена работа с внутренними пользователями:
  - Теперь вы можете добавлять учетные записи внутренних пользователей на портале.
  - Приложение теперь не позволяет вам сокращать свои собственные права.

Обновление от 18 октября 2021

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие новые функции и улучшения:

- Kaspersky Security Center Cloud Console теперь поддерживает продукт Kaspersky Endpoint Detection and Response Optimum 2.0.
- Теперь вы можете управлять мобильными устройствами с операционной системой Android с помощью Kaspersky Security Center Cloud Console.
- Kaspersky Marketplace доступен в виде нового раздела меню: теперь вы можете искать приложения "Лаборатории Касперского" с помощью Kaspersky Security Center Cloud Console.
- Доступен новый раздел Объявления "Лаборатории Касперского". Объявления "Лаборатории Касперского" информируют вас о приложениях "Лаборатории Касперского", установленных на управляемых устройствах. Kaspersky Security Center Cloud Console периодически обновляет информацию в этом разделе.
- Теперь вы можете управлять подчиненными Серверами администрирования, работающими на операционных системах Linux, через Kaspersky Security Center Cloud Console.

Обновление от 7 сентября 2021

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие новые функции и улучшения:

- Теперь вы можете использовать Active Directory Federation Services (AD FS) для входа в Kaspersky Security Center Cloud Console, используя свою учетную запись Active Directory и не создавая учетной записи.
- Kaspersky Security Center Cloud Console теперь работает со следующими облачными окружениями: Amazon Web Services, Microsoft Azure и Google Cloud. Для защиты виртуальных машин (или инстансов) в облачном окружении вам потребуется одна из лицензий Kaspersky Security для виртуальных и облачных сред. Доступен мастер настройки для работы в облачном окружении.
- Максимальное количество устройств на одну рабочую область теперь составляет 25 000.

- Теперь в Kaspersky Security Center Cloud Console доступна интеграция с SIEM-системами. Вы можете экспортировать события в SIEM-системы, используя формат Syslog.

- Теперь вы можете создавать виртуальные Серверы администрирования. Каждый виртуальный Сервер администрирования может иметь свою структуру групп администрирования, политик, задач, отчетов и событий. Вы можете использовать виртуальные Серверы администрирования для управления клиентскими организациями со сложными рабочими процессами в вашей рабочей области. Вы не можете перенести виртуальные Серверы администрирования из Kaspersky Security Center, работающего локально, в Kaspersky Security Center Cloud Console.

- Теперь вы можете настраивать ширину столбцов в таблицах, сортировать и искать данные.

- Улучшена стабильность работы и доступность Kaspersky Business Hub и Kaspersky Security Center Cloud Console.

Обновление от 27 октября 2020

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие новые функции и улучшения:

- Kaspersky Security Center Cloud Console теперь поддерживает Kaspersky Endpoint Security 11.6.0 для Windows, Kaspersky Endpoint Security 11.1 для Mac Patch A и Kaspersky Endpoint Agent 3.10 (в составе Kaspersky Endpoint Detection and Response Optimum).

- Вы можете использовать следующие лицензии:

  - Kaspersky Endpoint Detection and Response Optimum

  - Kaspersky Endpoint Security для бизнеса Расширенный

  - Kaspersky Total Security для бизнеса

- Внедрены следующие функции:

  - Системное администрирование

  - Управление шифрованием

  - Контроль приложений

  - Адаптивный контроль аномалий

  - RDP-сеансов, включая функцию совместного доступа к рабочему столу Windows

- Меню навигации теперь вертикальное, что напоминает интерфейс Консоли администрирования Kaspersky Security Center на основе консоли управления Microsoft Management Console (MMC).

- Теперь доступны обучающие видеоролики; они помогут вам узнать, как работает приложение.

Обновление от 30 июня 2020

Это обновление приложения Kaspersky Security Center Cloud Console включает следующие новые функции и улучшения:

- Kaspersky Security Center Cloud Console поддерживает Kaspersky Security 11 для Windows Server (с сентября 2020).
- Kaspersky Security Center Cloud Console поддерживает Kaspersky Endpoint Agent 3.9 и Kaspersky Endpoint Security 11.4.0 для Windows.
- Улучшен мастер первоначальной настройки: некоторые шаги были удалены, изменена последовательность шагов, некоторые тексты были изменены для удобства и простоты.
- Приложение Kaspersky Security Center Cloud Console теперь доступна на итальянском языке.
- Теперь вы можете отозвать Лицензионное соглашение для любым управляемым приложением "Лаборатории Касперского" с помощью интерфейса Kaspersky Security Center Cloud Console. Вам нужно удалить выбранное приложение, прежде чем отзывать его Лицензионное соглашение.
- Теперь вы можете удалять рабочие области. Если вы отмечаете рабочую область для удаления, она по умолчанию автоматически удаляется через семь дней. Также вы можете принудительно удалить рабочую область, чтобы она была немедленно удалена.
- Для входа в консоль реализована двухфакторная аутентификация.

Исправленные ошибки

В таблице ниже перечислены все проблемы, обнаруженные в предыдущих обновлениях Kaspersky Security Center Cloud Console и исправленные в текущем обновлении.

Список проблем, исправленных в Kaspersky Security Center Cloud Console

Обновление Kaspersky Security Center Cloud Console, в котором впервые возникла ошибка	Идентификатор ошибки	Описание проблемы
Обновление от февраля 2026	9526104	Исправлена ошибка, из-за которой текст всплывающей подсказки сливался с фоном при выборе мобильных сертификатов.
Обновление от июня 2026	9577592	Исправлена ошибка, из-за которой большие политики безопасности Kaspersky Endpoint Security могли некорректно загружать раздел **Параметры приложения**, в результате чего этот раздел мог отображаться пустым.
Обновление от июня 2026	10065748	Исправлена ошибка, из-за которой подробная информация о правиле при просмотре отчета **Отчет о работе Веб-Контроля** в Web Console не отображалась, если его название содержало квадратные скобки.
Обновление от июня 2026	10112458	Исправлена ошибка, из-за которой в полях **Ограничения пробной версии** и **Ограничения функций приложения** отсутствовала информация об ограничениях инсталляционных пакетов.
Обновление от июня 2026	10117987	Исправлена ошибка, из-за которой раздел **Сервер администрирования** в главном меню отображался на английском языке во всех локализациях.
Обновление от июня 2026	10128693	Исправлена ошибка, из-за которой появлялось сообщение **Произошла ошибка** при сохранении политики после внесения изменений.
Обновление от июня 2026	10128748	Исправлена ошибка, из-за которой в списке приложений отображались некорректные приложения Unified Protection and Management Plug-in при создании задачи **Запуск и остановка приложения**.
Обновление от июня 2026	10183311	Исправлена ошибка, из-за которой задача **Поиск уязвимостей и требуемых обновлений** могла завершаться со статусом **Завершена с предупреждением**.
Обновление от июня 2026	10189276	Исправлена ошибка, из-за которой установленное ограничение на количество групп безопасности могло применятся неправильно.
Обновление от июня 2026	10189594	Исправлена ошибка, из-за которой раздел **Панель мониторинга** вместе с иерархией групп администрирования отображался некорректно, если вы переходили в раздел **Задачи** из раздела **Панель мониторинга**, вручную изменив веб-адрес в браузере.
Обновление от февраля 2026	9501104	Исправлена ошибка, из-за которой обучающие материалы в соответствующем разделе могли запускаться не с первой попытки.
Обновление от июня 2026	9968154	Исправлена ошибка, из-за которой уведомления могли отображаться на неправильном языке после изменения языка интерфейса Web Console.
Обновление от июня 2026	10076008	Исправлена ошибка, из-за которой светлая тема могла на мгновение появиться при переходе между разделами во время загрузки страницы.
Обновление от июня 2026	10076016	Исправлена ошибка, из-за которой пользователь, чьи права доступа были только что отозваны, по-прежнему мог загрузить отчет об использовании лицензионных ключей, содержащий актуальные данные.
Обновление от июня 2026	10112524	Исправлена ошибка, из-за которой ненужный параметр `ui_locales` отображался в веб-адресе после переключения языка локализации.
Обновление от июня 2026	10126364	Исправлена ошибка, из-за которой вы могли переключиться с коммерческой лицензии на пробную.
Обновление от июня 2026	10128638	Исправлена ошибка, из-за которой после назначения пользовательских прав какому-либо пользователю, в свойствах группы администрирования пользователь мог некорректно отображаться в разделе **Пользователи и роли** → **Роли**.

Обновление от июня 2026	10146377	Исправлена ошибка, из-за которой если раздел MDR был установлен в качестве домашней страницы, он оставался домашней страницей даже после того, как параметр **Показать функции MDR** был выключен в разделе **Параметры** → **Параметры интерфейса**.
Обновление от июня 2026	10157485	Исправлена ошибка, из-за которой данные из раздела **Уязвимости в приложениях** некорректно экспортировались в форматы CSV и TXT.

Kaspersky Security Center Cloud Console

Приложение Kaspersky Security Center Cloud Console адресовано администраторам сетей организаций и сотрудникам, отвечающим за защиту устройств в организациях. Оно предоставляет широкие возможности для защиты устройств ваших пользователей и рекомендуется для крупных организаций. Kaspersky Security Center Cloud Console размещается и поддерживается в инфраструктуре "Лаборатории Касперского". Вам не нужно устанавливать Kaspersky Security Center Cloud Console на свой компьютер или сервер.

Kaspersky Security Center Cloud Console позволяет сделать следующее:

- Устанавливать приложения "Лаборатории Касперского" на устройства вашей сети и управлять установленными приложениями.
- Формировать иерархию групп администрирования для управления набором клиентских устройств как единым целым.
- Создавать виртуальные Серверы администрирования и располагать их в иерархии.
- Защищать свои сетевые устройства, включая рабочие станции и серверы:
  - Управлять системой защиты, построенной на основе приложений "Лаборатории Касперского".
  - Использовать возможности обнаружения и реагирования (EDR и MDR) (требуется лицензия на Kaspersky Endpoint Detection and Response и/или на Kaspersky Managed Detection and Response), включая:
    - анализ и исследование инцидентов;
    - визуализацию инцидентов с помощью построения графика цепочки развития угроз;
    - принятие или отклонение ответов вручную или настройка автоматического принятия всех ответов.
- Kaspersky Security Center Cloud Console представляет собой мультитенантное приложение.
- Удаленно управлять установленными приложениями "Лаборатории Касперского" на клиентских устройствах.
- Централизованно распространять лицензионные ключи приложений "Лаборатории Касперского" на клиентские устройства.
- Создавать и контролировать политики безопасности для устройств в вашей сети.
- Создавать и контролировать учетные записи пользователей.
- Создавать и управлять ролями пользователей (RBAC).
- Создавать и контролировать задачи приложений, установленных на устройствах сети.
- Просматривать отчеты о состоянии системы защиты для каждой организации индивидуально.

Перед использованием Kaspersky Security Center Cloud Console необходимо создать учетную запись и рабочую область.

Вы управляете Kaspersky Security Center Cloud Console с помощью Web Console, которая обеспечивает взаимодействие между вашим устройством и Сервером администрирования через браузер. Сервер администрирования – это приложение, которое служит для управления приложениями "Лаборатории Касперского", установленными на устройства вашей сети. Когда вы с помощью браузера подключаетесь к Kaspersky Security Center Cloud Console, браузер устанавливает с Сервером Kaspersky Security Center Cloud Console защищенное (HTTPS) соединение.

Сервер администрирования и подключенная система управления базами данных (СУБД) разворачиваются в облачном окружении и предоставляются вам в качестве службы. Обслуживание как Сервера администрирования, так и СУБД осуществляется в рамках сервиса. Все программные компоненты Kaspersky Security Center Cloud Console всегда актуальны. Сервер администрирования и созданные объекты, такие как политики и задачи, регулярно сохраняются для обеспечения их безопасности.

Kaspersky Security Center Cloud Console представляет собой многоязыковое приложение. Вы можете изменить язык интерфейса в любое время без повторного открытия приложения.

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

Аппаратные и программные требования Kaspersky Security Center Cloud Console

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.

Консоль администрирования

Для работы с Kaspersky Security Center Cloud Console требуется только браузер.

Вы можете использовать только одно окно или вкладку браузера для работы с Kaspersky Security Center Cloud Console.

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 Cloud Console.

Браузеры:

- Google Chrome версии 145.0.7632.26 или выше
- Microsoft Edge версии 145.0.3800.65 или выше
- Safari 18.6 в macOS
- Mozilla Firefox Extended Support Release версии 140.7.1.2 или выше

Агент администрирования

Минимальные аппаратные требования:

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

Минимальные требования для Системного администрирования:

- Процессор с частотой 1.4 ГГц или выше. Требуется 64-разрядная операционная система.
- Оперативная память: 8 ГБ.
- Объем свободного места на диске: 1 ГБ.

Архитектура Arm не поддерживается.

Операционные системы. Рабочие станции Microsoft Windows	Microsoft Windows Embedded POSReady 2009 с последним Service Pack 32-разрядная. Microsoft Windows Embedded 7 Standard Service Pack 1 32-разрядная/64-разрядная. Microsoft Windows Embedded 8.1 Industry Pro 32-разрядная/64-разрядная. Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная/64-разрядная. Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная/64-разрядная. Microsoft Windows 10 IoT Enterprise 2015 LTSB 32-разрядная/64-разрядная. Microsoft Windows 10 IoT Enterprise 2016 LTSB 32-разрядная/64-разрядная. Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная/64-разрядная. Microsoft Windows 10 IoT Enterprise версия 1703, 1709, 1803, 1809 32-разрядная/64-разрядная. Microsoft Windows 10 20H2, 21H2 IoT Enterprise 32-разрядная/64-разрядная. Microsoft Windows 10 IoT Enterprise 32-разрядная/64-разрядная. Microsoft Windows 10 IoT Enterprise версия 1909 32-разрядная/64-разрядная. Microsoft Windows 10 IoT Enterprise LTSC 2021 32-разрядная/64-разрядная. Microsoft Windows 10 IoT Enterprise версия 1607 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 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 8.1 Pro/Enterprise 32-разрядная/64-разрядная. Microsoft Windows 8 Pro/Enterprise 32-разрядная/64-разрядная. Microsoft Windows 7 Home/Pro/Enterprise/Ultimate Service Pack 1 и выше 32-разрядная/64-разрядная. Microsoft Windows XP Professional Service Pack 3 и выше 32-разрядная (поддерживается Агентом администрирования версии 14.0.0.20023, требуется Security Update for Windows XP KB2868626). Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32-разрядная (поддерживается Агентом администрирования версии 14.0.0.20023).

Операционные системы. Серверы Microsoft Windows	Microsoft Windows MultiPoint Server 2011 Standard/Premium 64-разрядная. Microsoft Windows Server 2008 Standard/Enterprise/Datacenter/Foundation Service Pack 2 32-разрядная/64-разрядная. Microsoft Windows Server 2008 R2 Standard/Datacenter/Enterprise/Foundation with 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. Microsoft Windows Server 2016 Server Core/Datacenter/Essentials/Standard (вариант установки Server Core) (LTSB) 64-разрядная. Microsoft Windows Server 2019 Standard/Datacenter/Core 64-разрядная. Microsoft Windows Server 2019 RS5 Essentials/Standard 64-разрядная. Microsoft Windows Server 2022 Standard/Datacenter/Core 64-разрядная. Microsoft Windows Server 2022 21H2 Standard/Datacenter 64-разрядная. Microsoft Windows Server 2025 Standard/Datacenter/Core 64-разрядная. Microsoft Windows Small Business Server 2011 Standard/Essentials/Premium Add-on 64-разрядная.
Операционные системы. Linux	Debian GNU/Linux 13 (Trixie) 64-разрядная. Debian GNU/Linux 12 (Bookworm) 32-разрядная/64-разрядная. Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная. Ubuntu Server 24.04 LTS 64-разрядная. Ubuntu Server 22.04 LTS 64-разрядная. Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная. CentOS 7.x 64-разрядная. CentOS Stream 10 64-разрядная. CentOS Stream 9 64-разрядная. CentOS Stream 8 64-разрядная. Red Hat Enterprise Linux Server 10.x 64-разрядная. Red Hat Enterprise Linux Server 9.x 64-разрядная. Red Hat Enterprise Linux Server 8.x 64-разрядная. Red Hat Enterprise Linux Server 7.x 64-разрядная. openSUSE Leap 15 64-разрядная. SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная. SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная. Oracle Linux 7 64-разрядная. Oracle Linux 8 64-разрядная. Oracle Linux 9 64-разрядная. Linux Mint 21.x 64-разрядная. Linux Mint 22.x 64-разрядная. Alma Linux 8.x 64-разрядная. Alma Linux 9.x 64-разрядная. Rocky Linux 8.x 64-разрядная. Rocky Linux 9.x 64-разрядная. Amazon Linux 2 64-разрядная. Kylin 10 64-разрядная.
Операционные системы. macOS	Список поддерживаемых операционных систем см. в справке Kaspersky Endpoint Security для Mac.

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

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

Перед установкой Агента администрирования на устройства под управлением Windows 7, Windows Server 2008 или Windows Server 2008 R2 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 (KB3063858), Обновление безопасности для Windows Server 2008 x64 Edition (KB3063858), Обновление безопасности для Windows Server 2008 R2 x64 Edition (KB3063858).

Совместимые приложения и решения "Лаборатории Касперского"

Лицензии на разные приложения предоставляют разные наборы приложений и решений "Лаборатории Касперского".

С помощью Kaspersky Security Center Cloud Console вы можете разворачивать следующие приложения и решения "Лаборатории Касперского" и управлять ими:

- Kaspersky Endpoint Security 14.1 для Windows (поддерживается только Lite encryption (AES56))
- Kaspersky Endpoint Security 12.5 для Linux
- Kaspersky Endpoint Security 12.2 для Mac
- Kaspersky Embedded Systems Security 4.0 для Windows
- Kaspersky Embedded Systems Security 4.0 для Linux
- Kaspersky Endpoint Agent 4.0
- Kaspersky Endpoint Security для Android
- Kaspersky Security для iOS

Вы можете интегрировать следующие решения для просмотра и обработки инцидентов безопасности:

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

- Kaspersky Symphony XDR
- Kaspersky Security для бизнеса Профессиональный

Если вы устанавливаете на управляемом устройстве новую версию приложения, но не обновили политику для него, то приложение все равно передает данные в Kaspersky Security Center Cloud Console, но Kaspersky Security Center Cloud Console не может обработать данные так, как описано в разделе "Обрабатываемые данные управляемых приложениях". Чтобы Kaspersky Security Center Cloud Console обрабатывал эти данные, вам нужно создать политику для новой версии приложения.

Локализация приложения Kaspersky Security Center Cloud 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.

Сравнение Kaspersky Security Center и Kaspersky Security Center Cloud Console

Вы можете использовать Kaspersky Security Center следующими способами:

- Как облачное решение.

  Приложение Kaspersky Security Center устанавливается 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.

- Как локальное решение (для Windows или Linux).

  Вы устанавливаете Kaspersky Security Center на локальное устройство и управляете системой безопасности сети с помощью Консоли администрирования на основе консоли управления Microsoft Management Console (MMC) или с помощью Kaspersky Security Center Web Console.

  Помимо приложения для Windows, также доступно приложение Kaspersky Security Center Linux. Kaspersky Security Center Linux предназначен для развертывания и управления защитой устройств с операционной системой Linux с помощью Сервера администрирования на базе Linux в соответствии с требованиями чистых сред Linux. Kaspersky Security Center Windows и Kaspersky Security Center Linux имеют разный набор функций.

Приведенная ниже таблица позволяет сравнить основные функции Kaspersky Security Center и Kaspersky Security Center Cloud Console.

Сравнение возможностей приложения Kaspersky Security Center, работающего локально и как облачное решение

Функция или свойство	Приложение Kaspersky Security Center, работающее локально	Kaspersky Security Center Cloud Console
Расположение Сервера администрирования	В локальной инфраструктуре	Облачное окружение
Расположение системы управления базами данных (СУБД)	В локальной инфраструктуре	Облачное окружение
Веб-версия Консоли администрирования	✓	✓
Обслуживание Сервера администрирования и СУБД	Управляется администратором	Управляется "Лабораторией Касперского"
Иерархия Серверов администрирования	✓	✓ Сервер администрирования Kaspersky Security Center Cloud Console может выступать только в качестве главного Сервера администрирования в иерархии и может использоваться только для политик и задач мониторинга.
Иерархия групп администрирования	✓	✓
Перенос данных управляемых устройств и связанных с ними объектов из локального Kaspersky Security Center в Kaspersky Security Center Cloud Console	✓	✓
Опрос сети	✓	✓ (только точками распространения)
Максимальное количество управляемых устройств	100 000	25 000

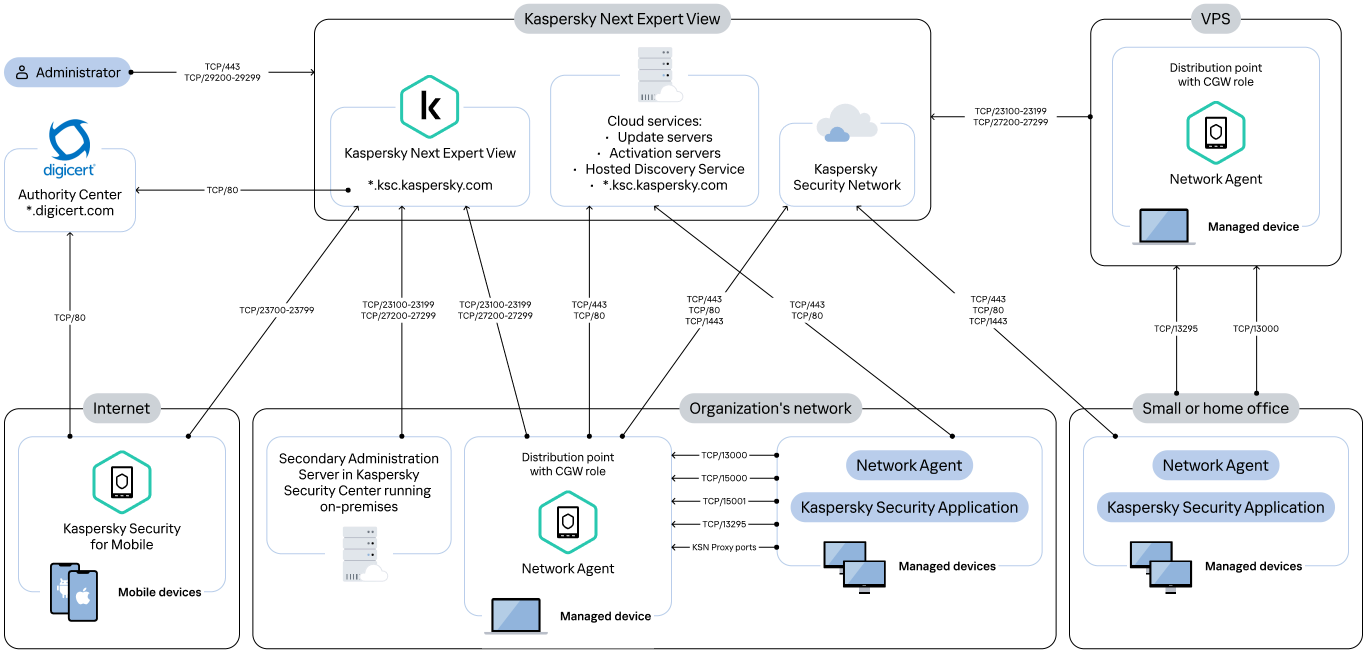
Функция или свойство	Приложение Kaspersky Security Center, работающее локально	Kaspersky Security Center Cloud Console
Защита устройств под управлением Windows, Linux и macOS	✓	✓
Защита мобильных устройств	✓	✓ (поддерживаются только Kaspersky Endpoint Security for Android и Kaspersky Security for iOS)
Защита публичной облачной инфраструктуры	✓	✓
Управление безопасностью устройств	✓	✓
Политики приложений	✓	✓
Задачи для приложений "Лаборатории Касперского"	✓	✓
Kaspersky Security Network	✓	✓
Прокси-сервер KSN	✓	✓ (только на точках распространения)
Kaspersky Private Security Network	✓	—
Централизованное распространение лицензионных ключей приложений "Лаборатории Касперского"	✓	✓
Переключение управляемых устройств на другой Сервер администрирования	✓	— (необходимо переустановить Агенты администрирования на управляемых устройствах, чтобы переключить их на другой Сервер администрирования)
Поддержка виртуальных Серверов администрирования	✓	✓
Установка обновлений приложений сторонних производителей и поиск уязвимостей в приложениях сторонних производителей	✓	✓ (для закрытия уязвимостей в приложениях сторонних производителей устанавливать можно только рекомендованные исправления)
Уведомления о событиях, произошедших на управляемых устройствах	✓	✓
Создание учетных записей пользователей, контроль учетных записей	✓	✓
Максимальное количество событий в базе данных	400 000 (можно увеличить до 45 000 000)	400 000
Интеграция с SIEM-системами	✓	✓ (только с использованием формата Syslog и TLS over TCP)
Использовать Сервер администрирования в роли WSUS-сервера	✓	—
Мониторинг статусов политик и задач	✓	✓
Поддержка кластеров и массивов серверов в группах администрирования	✓	✓
Удаленная установка операционных систем	✓	—
Поддержка SNMP	✓	—
Максимальное количество виртуальных Серверов	500	200
Клонирование жесткого диска устройства	✓	—
Поддержка OpenAPI	✓	—

Архитектура и основные понятия

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

Архитектура

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



Архитектура приложения Kaspersky Security Center Cloud Console

Приложение Kaspersky Security Center Cloud Console, управляемое с помощью консоли на основе облачной службы, включает два основных компонента: инфраструктура Kaspersky Security Center Cloud Console и инфраструктура клиента.

Инфраструктура Kaspersky Security Center Cloud Console содержит:

- **Консоль администрирования на основе облачной службы**. Представляет собой веб-интерфейс для создания и управления системой защиты сети организации-клиента, находящейся под управлением Kaspersky Security Center Cloud Console.

- **Облачные сервисы**. Включает в себя серверы обновлений и серверы активации.

- **Kaspersky Security Network (KSN)**. Серверы, которые содержат оперативные базы 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.

Инфраструктура клиента может содержать следующее:

- **Точку распространения**. Устройство с установленным Агентом администрирования, которое используется для распространения обновлений, удаленной установки приложений, получения информации об устройствах в составе группы администрирования и/или широковещательного домена. 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.

- **Управляемые устройства**. Компьютеры сети клиента, защищенные с помощью Kaspersky Security Center Cloud Console. Агент администрирования и приложение безопасности "Лаборатории Касперского" должны быть установлены на каждом управляемом устройстве.

- **Подчиненный Сервер администрирования, работающий локально** (необязателен). Вы можете использовать Сервер администрирования, работающий локально, для создания иерархии Серверов администрирования.

Порты, используемые Kaspersky Security Center Cloud Console

Чтобы использовать Kaspersky Security Center Cloud Console, который является частью инфраструктуры "Лаборатории Касперского", необходимо открыть следующие порты на клиентских устройствах, чтобы разрешить на них подключение к интернету (см. таблицу ниже):

Порты, которые должны быть открыты на клиентских устройствах для подключения к интернету

Порт (или диапазон портов)	Протокол	Назначение порта (или диапазона портов)
23100–23199	TCP/TLS	Прием подключений от Агентов администрирования и подчиненных Серверов администрирования на Сервере администрирования Kaspersky Security Center Cloud Console по адресу *.ksc.kaspersky.com. Инфраструктура "Лаборатории Касперского" может использовать любой порт из этого диапазона и любой веб-адрес в пределах этой маски. Порт и веб-адрес могут время от времени меняться.
23700–23799 (только если вы управляете мобильными устройствами)	TCP/TLS	Прием подключений от мобильных устройств. Подключение к Серверу администрирования Kaspersky Security Center Cloud Console по адресу *.ksc.kaspersky.com. Инфраструктура "Лаборатории Касперского" может использовать любой порт из этого диапазона и любой веб-адрес в пределах этой маски. Порт и веб-адрес могут время от времени меняться.
27200–27299	TCP/TLS	Прием подключений для активации приложений от управляемых устройств (кроме мобильных устройств). Подключение к Серверу администрирования Kaspersky Security Center Cloud Console по адресу *.ksc.kaspersky.com. Инфраструктура "Лаборатории Касперского" может использовать любой порт из этого диапазона и любой веб-адрес в пределах этой маски. Порт и веб-адрес могут время от времени меняться.
29200–29299	TCP/TLS	Туннелирование подключений к управляемым устройствам с помощью утилиты klsctunnel через Сервер администрирования Kaspersky Security Center Cloud Console по адресу *.ksc.kaspersky.com. Инфраструктура "Лаборатории Касперского" может использовать любой порт из этого диапазона и любой веб-адрес в пределах этой маски. Порт и веб-адрес могут время от времени меняться.
443	HTTPS	Подключение к службе обнаружения Kaspersky Security Center Cloud Console по адресу *.ksc.kaspersky.com. Инфраструктура "Лаборатории Касперского" может использовать любой веб-адрес в пределах этой маски.

Порт (или диапазон портов)	Протокол	Назначение порта (или диапазона портов)
1443	TCP	Подключение к Kaspersky Security Network.
80	TCP	Соединение используется для проверки срока действия сертификатов Kaspersky Security Center на *.digicert.com. Инфраструктура "Лаборатории Касперского" может использовать любой веб-адрес в пределах этой маски.

В таблице ниже указаны порты, которые должны быть открыты на клиентских устройствах, на которых установлен Агент администрирования.

Порты, которые должны быть открыты на клиентских устройствах

Номер порта	Протокол	Назначение порта	Область
15000	UDP	Получение данных от шлюзов соединения (если они используются)	Управление клиентскими устройствами
15000	Широковещательная рассылка UDP	Получение данных о других Агентах администрирования в пределах одного широковещательного домена	Доставка обновлений и инсталляционных пакетов
15001	UDP	Получение многоадресных запросов от точек распространения (если используется)	Получение обновлений и инсталляционных пакетов от точки распространения

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 Cloud Console 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 дополнительные порты, которые должны быть открыты на клиентских устройствах с установленным Агентом администрирования, выполняющим роль точки распространения.

Порты, используемые Агентом администрирования, который работает в качестве точки распространения

Номер порта	Протокол	Назначение порта	Область
13000	TCP/TLS	Прием подключений от Агентов администрирования	Управление клиентскими устройствами, доставка обновлений и инсталляционных пакетов
13111 (только если на устройстве запущена служба прокси-сервера KSN)	TCP	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN
13295 (только если вы используете точку распространения в качестве push-сервера)	TCP/TLS	Отправка push-уведомлений управляемым устройствам	Точка распространения используется как push-сервер
15111 (только если на устройстве запущена служба прокси-сервера KSN)	UDP	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN
17111 (только если на устройстве запущена служба прокси-сервера KSN)	HTTPS	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN

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	Только для клиентских устройств с операционными системами Linux. Удаленная установка приложений "Лаборатории Касперского" с помощью точки распространения с операционной системой Linux.

Если у вас есть один или несколько Серверов администрирования в вашей сети и вы используете их в качестве подчиненных Серверов администрирования, когда главный Сервер администрирования расположен в инфраструктуре "Лаборатории Касперского", обратитесь к списку портов, которые используются Kaspersky Security Center и Kaspersky Security Center Linux, работающим локально. Используйте эти порты для взаимодействия вашего подчиненного Сервера администрирования (или подчиненных Серверов администрирования) и клиентских устройств.

Основные понятия

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

Агент администрирования

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

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

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

Устройство, на которое установлен Агент администрирования, называется *управляемым устройством* или *устройством*. Агент администрирования можно установить на устройство под управлением операционной системы Windows, Linux или Mac.

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

Агент администрирования синхронизирует управляемое устройство с Сервером администрирования. Kaspersky Security Center Cloud Console автоматически синхронизирует Сервер администрирования с управляемыми устройствами несколько раз в час. Сервер администрирования устанавливает период синхронизации (англ. *heartbeat*) в зависимости от количества 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 Cloud Console.

Для всех управляемых устройств в группе администрирования устанавливаются:

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

Управляемое устройство может входить в состав только одной группы администрирования.

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

Иерархия Серверов администрирования

Серверы администрирования могут образовывать иерархию вида "главный сервер – подчиненный сервер". Каждый Сервер администрирования может иметь несколько подчиненных Серверов администрирования на разных уровнях иерархии. Уровень вложенности подчиненных Серверов администрирования не ограничен. При этом в состав групп администрирования главного Сервера будут входить клиентские устройства всех подчиненных Серверов.

Сервер администрирования Kaspersky Security Center Cloud Console может выступать только в качестве главного Сервера администрирования и иметь в качестве подчиненных Серверов только Серверы администрирования, работающие локально.

При переносе данных с Сервера администрирования, который работает локально, на Сервер администрирования Kaspersky Security Center Cloud Console вы можете расположить Серверы администрирования в иерархии. Затем для уменьшения рисков при переносе данных вы можете переключить только часть ваших управляемых устройств под управление Сервера администрирования Kaspersky Security Center Cloud Console. Остальные управляемые устройства остаются под управлением локального Сервера администрирования. Это позволит протестировать функции управления Kaspersky Security Center Cloud Console на ограниченном количестве управляемых устройств. В то же время вы можете настроить политики, задачи, отчеты и другие объекты для тестирования управления и контроля всей вашей сети. Это позволит при необходимости вернуться к объектам, настроенным на локальном Сервере администрирования.

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

Виртуальный Сервер администрирования

Виртуальный Сервер администрирования (далее также *виртуальный Сервер*) – компонент приложения Kaspersky Security Center Cloud Console, предназначенный для управления антивирусной защитой сети организации-клиента. Каждый виртуальный Сервер администрирования может иметь свою структуру групп администрирования и собственные средства управления и мониторинга, такие как политики, задачи, отчеты и события. Функциональные возможности виртуальных Серверов администрирования могут использоваться организациями со сложными рабочими процессами.

Виртуальный Сервер администрирования имеет следующие ограничения:

- Виртуальные Серверы администрирования поддерживаются только в коммерческом режиме приложения Kaspersky Security Center Cloud Console.
- Для виртуального Сервера не поддерживается создание подчиненных Серверов администрирования (в том числе и виртуальных).
- Вы не можете перенести виртуальные Серверы администрирования из Kaspersky Security Center в Kaspersky Security Center Cloud Console.
- По умолчанию администратор, управляющий главным Сервером администрирования, также управляет всеми виртуальными Серверами администрирования.
- Пользователям, которые были созданы на виртуальном Сервере, невозможно назначить роли на Сервере администрирования.
- В окне свойств виртуального Сервера ограничен набор разделов.

Точка распространения

Точка распространения – это устройство с установленным Агентом администрирования, который используется для распространения обновлений, удаленной установки приложений, получения информации об устройствах в сети. Точки распространения также могут выступать в качестве шлюзов соединения для уменьшения количества исходящих внешних подключений и количества одновременных подключений к Серверу администрирования.

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, на клиентские устройства группы (в том числе и с помощью широковещательной рассылки по протоколу UDP). Обновления могут быть получены с серверов обновлений "Лаборатории Касперского" с помощью задачи обновления, созданной для точки распространения.

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

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

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

- Выполнять роль шлюза соединений с Сервером администрирования, так как в облачной инфраструктуре часто невозможно установить прямое соединение устройств сети с Сервером администрирования. Шлюз соединений оптимизирует сетевые соединения и снижает нагрузку на Сервер администрирования.

- Опрашивать сеть с целью обнаружения новых устройств и обновления информации об уже известных устройствах.

- Выполнять удаленную установку как сторонних приложений, так и приложений "Лаборатории Касперского" средствами Microsoft Windows, в том числе на клиентские устройства без установленного 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.

- Исполнять роль прокси-сервера, участвующего в Kaspersky Security Network.

  Такая возможность не поддерживается для точек распространения под управлением macOS.

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 (ksnproxy).

Если у вас более 10 000 устройств, несколько виртуальных Серверов и политик, настоятельно рекомендуется использовать точки распространения для правильного функционирования вашей инфраструктуры. При назначении устройства точкой распространения см. статью Расчет количества и конфигурации точек распространения.

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 уменьшения трафика.

Областью действия точки распространения является одна или несколько групп администрирования, для которых она назначена администратором, а также ее подгруппы всех уровней вложенности. При этом устройство, являющееся точкой распространения, не обязано находиться в группе администрирования, на которую она назначена. Если в иерархии групп администрирования назначено несколько точек распространения, Агент администрирования управляемого устройства подключается к наиболее близкой по иерархии точке распространения.

Областью действия точек распространения также может являться одно или несколько сетевых местоположений. Сетевые местоположения используются для формирования вручную набора устройств, на которые точка распространения будет распространять обновления. Определение сетевого местоположения доступно для устройств под управлением операционной системы Windows и Linux.

Kaspersky Security Center Cloud Console присваивает каждому Агенту администрирования уникальный адрес многоадресной IP-рассылки, который не пересекается с другими адресами. Это позволяет избежать превышения нагрузки на сеть, которое возникло бы из-за пересечения адресов.

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

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

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 Cloud Console 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.

Веб-плагин управления

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

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 Cloud 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 Cloud Console предоставляет по одной политике для каждого приложения "Лаборатории Касперского" в группе администрирования. Политика имеет один из следующих статусов (см. таблицу ниже):

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.

- Вы можете активировать неактивную политику при возникновении определенного события. Например, в период вирусных атак можно включить параметры для усиленной антивирусной защиты.

- Политика может иметь дочерние политики.

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

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

Профиль политики – это именованное подмножество параметров политики, которые заменяют значения параметров политики. Профиль политики влияет на формирование эффективных параметров управляемого устройства. *Эффективные параметры* – это набор параметров политики, параметров профиля политики и параметров 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 Cloud Console 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.

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.

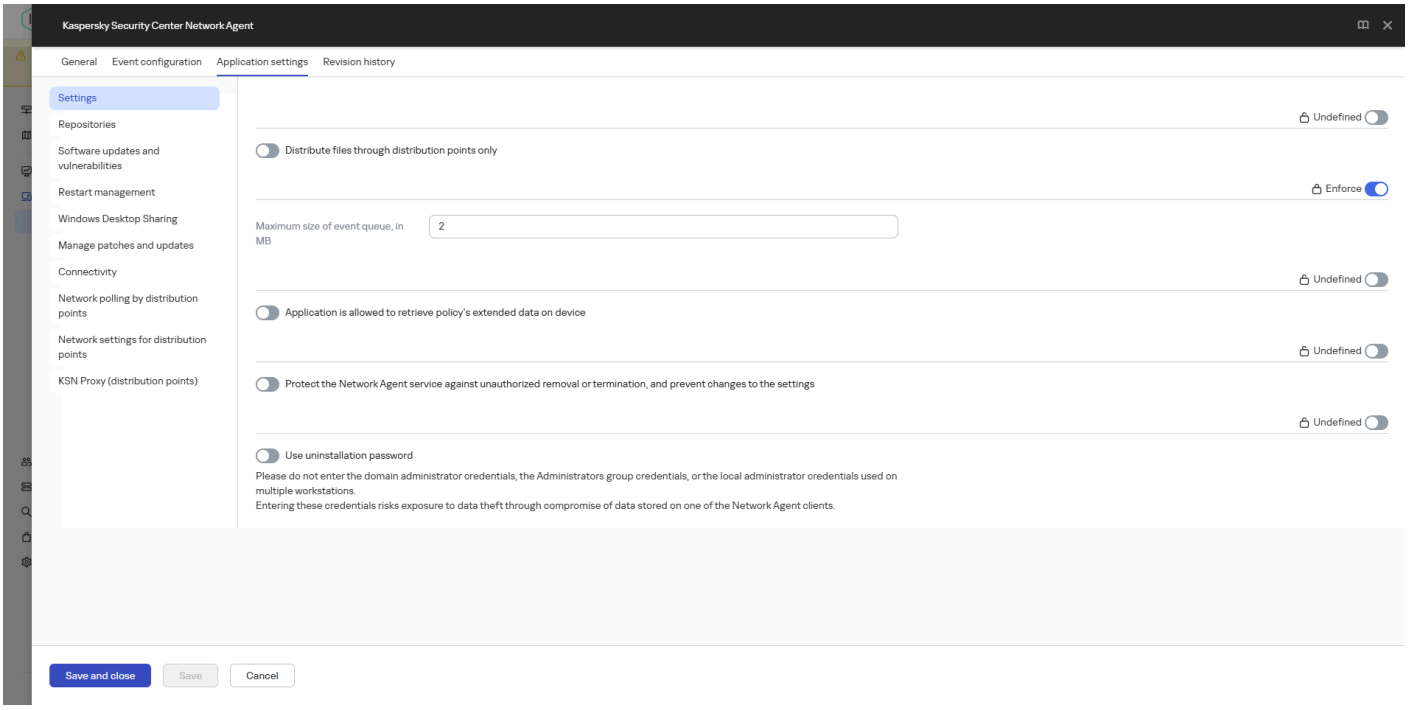
- Если запрет не наложен, то на каждом клиентском устройстве приложение использует локальное значение параметра, а не то, которое указано в политике. При этом значение параметра может изменяться через локальные параметры приложения.

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.



Параметры политики приложения

Лицензирование приложения

В этом разделе представлена информация, связанная с лицензированием приложения.

Лицензирование приложения Kaspersky Security Center Cloud Console

Следуя этому сценарию, вы можете приступить к использованию Kaspersky Security Center Cloud Console и управляемых приложений безопасности по лицензии.

Kaspersky Security Center Cloud Console позволяет централизованно распространять лицензионные ключи приложений "Лаборатории Касперского" на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.

Если вы уже используете Kaspersky Security Center Cloud Console, вы можете перейти в раздел Kaspersky Marketplace, который позволяет просмотреть весь спектр бизнес-решений "Лаборатории Касперского", выбрать те, которые нужны вам, и перейти к покупке на сайте "Лаборатории Касперского".

Ознакомление с функциями Kaspersky Security Center Cloud Console в пробном режиме перед покупкой лицензии

Вы можете сначала попробовать пробную версию Kaspersky Security Center Cloud Console. Для этого создайте пробную рабочую область, срок действия которой истекает через 30 дней. Если вам нужна коммерческая рабочая область, которую можно использовать столько, сколько нужно, вам нужно приобрести лицензию.

Этапы

Сценарий состоит из следующих этапов:

1. **Получение кода активации для лицензирования Kaspersky Security Center Cloud Console в коммерческом режиме. Приобретение лицензии (или лицензий)**

   Разные лицензии позволяют использовать разные приложения и службы "Лаборатории Касперского", поэтому вы можете приобрести несколько лицензий.

   Узнайте, какие лицензии вы можете приобрести и минимальное количество устройств для каждой лицензии.

   Kaspersky Security Center Cloud Console входит в состав нескольких решений "Лаборатории Касперского". Выберите, какое решение вы хотите использовать, и приобретите на него лицензию. Вам нужно будет обратиться в "Лабораторию Касперского" или к одному из партнеров "Лаборатории Касперского" с особым запросом, если вы хотите приобрести лицензию на 10 000 и более устройств.

   Используйте таблицу, чтобы проверить какие возможности Системного администрирования доступны в зависимости типа лицензии, по которой используется приложение.

Если вы хотите использовать Kaspersky Security Center Cloud Console в облачном окружении, таком как Microsoft Azure, прочитайте о вариантах лицензирования для облачных окружений.

Если вы являетесь поставщиком услуг (MSP), прочтите о лицензировании Kaspersky Security Center Cloud Console для поставщиков услуг.

2. **Активация Kaspersky Security Center Cloud Console при создании рабочей области**

   Вы указываете лицензионный ключ для активации Kaspersky Security Center Cloud Console при создании рабочей области.

   Если у вас несколько лицензионных ключей, укажите любой из них. Позже вам необходимо будет добавить другие лицензионные ключи в Kaspersky Security Center Cloud Console для активации управляемых приложений "Лаборатории Касперского".

3. **Добавление лицензионных ключей для управляемых приложений в хранилище Сервера администрирования**

   Перед развертыванием лицензионных ключей вам нужно добавить эти лицензионные ключи в хранилище Сервера администрирования.

   Лицензионный ключ, указанный вами при создании рабочей области, автоматически добавляется в хранилище Сервера администрирования.

   Если у вас более одного лицензионного ключа, добавьте лицензионные ключи по одному в хранилище Сервера администрирования Kaspersky Security Center Cloud Console.

4. **Распространение лицензионных ключей для управляемых приложений**

   Выберите способ распространения лицензионного ключа (или лицензионных ключей) на все устройства, которые вы хотите защитить:

   - Автоматическое распространение

     > Если вы используете разные управляемые приложения и вам важно распространить определенный код активации приложений, используйте другие способы распространения кода активации.

     Kaspersky Security Center позволяет автоматически распространять имеющиеся лицензионные ключи управляемых приложений. Например, в хранилище Сервера администрирования находится три лицензионных ключа. Вам нужно включить параметр **Автоматически распространять лицензионный ключ на управляемые устройства** для всех трех лицензионных ключей. На устройствах организации установлено приложение безопасности "Лаборатории Касперского", например, Kaspersky Endpoint Security для Windows. Обнаружено новое управляемое приложение на устройстве, для которого необходимо распространить лицензионный ключ. Например, приложение определяет, что для этого устройства подходит два лицензионных ключа из хранилища: лицензионный ключ *Ключ_1* и лицензионный ключ *Ключ_2*. Распространяется один из подходящих лицензионных ключей управляемого приложения. В этом случае невозможно предсказать, какой из этих двух лицензионных ключей будет распространен, так как автоматическое распространение лицензионных ключей не предполагает вмешательства администратора.

     При распространении лицензионного ключа на устройства происходит подсчет количества установок для данного лицензионного ключа. Вам необходимо удостовериться, что количество приложений, для которых распространяется лицензионный ключ, не превышает лицензионное ограничение. В случае если количество установок превышает лицензионное ограничение, таким устройствам будет присвоен статус *Критический*.

     Инструкции:

     - Добавление лицензионного ключа в хранилище Сервера администрирования.
     - Автоматическое распространение лицензионного ключа.

- 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.

  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.

5. **Проверка на каких устройствах активированы управляемые приложения "Лаборатории Касперского"**

   Чтобы убедиться, что лицензионные ключи распространены правильно, просмотрите список лицензионных ключей, которые используются для приложения.

6. **Настройка событий, связанных с истечением срока действия лицензии**

   Настройте события, чтобы получать уведомления, когда срок действия ваших лицензионных ключей истек или скоро истекает:

   - Критические события Сервера администрирования
   - События отказа функционирования Сервера администрирования
   - События предупреждения Сервера администрирования
   - Информационные события Сервера администрирования

О пробной версии Kaspersky Security Center Cloud Console

Пробная версия – это специальная версия Kaspersky Security Center Cloud Console, предназначенная для ознакомления пользователя с функциями Kaspersky Security Center Cloud Console. Когда вы начинаете использовать Kaspersky Security Center Cloud Console, вы можете запросить пробную рабочую область или ввести код активации коммерческой лицензии. Если запрашивается пробная рабочая область, 30-дневная пробная лицензия автоматически вступает в действие. В пробном режиме доступны те же функции, что и в приложении активированном по лицензии Kaspersky Next EDR Optimum.

Если приложение активировано по коммерческой лицензии до истечения срока действия пробной версии, конфигурация рабочей области и все ранее добавленные устройства сохраняются. Иначе рабочая область и все ее данные будут автоматически удалены по истечении пробного периода.

На использование функций пробной версии Kaspersky Security Center Cloud Console распространяются следующие ограничения:

- Невозможно создать иерархию Серверов администрирования. Невозможно создать виртуальные Серверы администрирования.
- Невозможно создать пользовательские инсталляционные пакеты.
- Вы не можете создавать пользовательские роли.
- Функция Вирусной атаки недоступна. События Вирусной атаки не хранятся и уведомления не отправляются.
- Хранилище **Удаленные объекты** недоступно.
- Невозможно включить добавление событий (опубликованных в больших количествах) в базу данных.
- Перенос данных Серверов администрирования из локального режима в режим Web Console не поддерживается.
- Статистическая информация KSN от компонентов Сервера администрирования, таких как Сервер администрирования или Агент администрирования, не отправляется в "Лабораторию Касперского".
- Интеграция со службами федерации Active Directory (AD FS) не поддерживается.
- Интеграция с Microsoft Entra ID не поддерживается.

Также накладываются ограничения на создание некоторых объектов приложения (см. таблицу ниже). Если создание объекта приводит к превышению какого-либо из этих ограничений, то операция будет заблокирована и появится сообщение об ошибке, сообщающее о превышении.

Ограничения на создание объектов Expert View в пробном режиме

Тип ограничения	Значение
Политики	30
Задачи.	30
Лицензионные ключи	5
Инсталляционные пакеты	8
Выборки устройств (предустановленные экземпляры не включены)	5
Выборки событий (предустановленные экземпляры не включены)	5
Правила перемещения устройств.	3
Шаблоны отчетов одного типа	10
Внутренние группы безопасности	20
Управляемые устройства	500

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 Cloud Console 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.

Лицензии и минимальное количество устройств для каждой лицензии

Если вы хотите использовать коммерческую версию приложения Kaspersky Security Center Cloud Console, перед созданием первой рабочей области вам нужно приобрести лицензию. В таблице ниже показаны лицензии, которые вы можете приобрести, и минимальное количество устройств для каждой лицензии (даже если вы хотите защитить меньшее количество устройств):

Лицензии, которые позволяют использовать Kaspersky Security Center Cloud Console

Лицензия	Минимальное количество устройств (даже если вы хотите защитить меньшее количество устройств)
Kaspersky Endpoint Security для бизнеса Стандартный	Для коммерческих лицензий: 300 Для коммерческих лицензий (по подписке): 100
Kaspersky Endpoint Security для бизнеса Расширенный	Для коммерческих лицензий: 300 Для коммерческих лицензий (по подписке): 100
Kaspersky Total Security для бизнеса.	300
Kaspersky Endpoint Detection and Response Optimum	Для коммерческих лицензий: 300 Для коммерческих лицензий (по подписке): 100
Kaspersky Endpoint Detection and Response Expert	50
Kaspersky Security для виртуальных и облачных сред, настольный компьютер	Для коммерческих лицензий: 300 Для коммерческих лицензий (по подписке): 100.
Kaspersky Security для виртуальных и облачных сред, сервер	50
Kaspersky Security для виртуальных и облачных сред, ядро	20
Kaspersky Security для виртуальных и облачных сред, процессор	20
Kaspersky Security для виртуальных и облачных сред Enterprise, настольный компьютер	Для коммерческих лицензий: 300 Для коммерческих лицензий (по подписке): 100.
Kaspersky Security для виртуальных и облачных сред Enterprise, сервер	50
Kaspersky Security для виртуальных и облачных сред Enterprise, процессор	20
Kaspersky Embedded Systems Security	300
Kaspersky Embedded Systems Security Compliance Edition	300
Kaspersky Symphony (в настоящее время доступно только в России)	300

Лицензия	Минимальное количество устройств (даже если вы хотите защитить меньшее количество устройств)
Kaspersky Next EDR Foundations	100 пользователей. Каждая лицензия может применяться к одному устройству PC/Mac и к двум мобильным устройствам.
Kaspersky Next EDR Optimum	100 пользователей. Каждая лицензия может применяться к одному устройству PC/Mac и к двум мобильным устройствам.
Kaspersky Next Complete Security	100 пользователей. Каждая лицензия может применяться к одному устройству PC/Mac и к двум мобильным устройствам.
Kaspersky Next EDR Expert	100 пользователей. Каждая лицензия может применяться к одному устройству PC/Mac и к двум мобильным устройствам.
Kaspersky Symphony XDR	100 пользователей. Каждая лицензия может применяться к одному устройству PC/Mac и к двум мобильным устройствам.
Kaspersky Next MXDR Optimum	150 пользователей.
Kaspersky XDR Optimum (в настоящее время доступно только в России и СНГ)	Для коммерческих лицензий: 300 пользователей. Для коммерческих лицензий (по подписке): 100 пользователей.
Kaspersky Security для бизнеса Профессиональный	100 пользователей. Каждая лицензия может применяться к одному устройству PC/Mac и к двум мобильным устройствам.

Если вы хотите защитить более 10 000 устройств, вам нужно отправить запрос в Службу технической поддержки "Лаборатории Касперского" и указать информацию о рабочей области, которую вы хотите создать.

События превышения лицензионного ограничения

Kaspersky Security Center Cloud Console 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**.

Способы распространения кодов активации на управляемые устройства

Приложения "Лаборатории Касперского" установленные на управляемых устройствах, должны быть активированы путем применения кода активации к каждой из приложений. Вы не можете использовать файлы ключей для лицензирования управляемых приложений; вы можете применять только коды активации. Код активации может быть распространен следующими способами:

- автоматическое распространение;
- с помощью задачи добавления лицензионного ключа управляемого приложения;
- активация управляемого приложения вручную.

Приложения "Лаборатории Касперского" могут использовать одновременно несколько лицензионных ключей. Например, Kaspersky Endpoint Security для Windows может использовать два лицензионных ключа: один для Kaspersky Endpoint Security для Windows и один для активации встроенных функций Endpoint Detection and Response.

Кроме того, приложения "Лаборатории Касперского" могут иметь не только активный лицензионный ключ, но и резервный лицензионный ключ. Приложение "Лаборатории Касперского" использует активный в данный момент ключ и сохраняет резервный ключ, который будет применяться после истечения срока действия активного ключа. Вы можете добавить активный или резервный лицензионный ключ любым из перечисленных выше способов. 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.

Добавление лицензионного ключа Сервера администрирования

Чтобы добавить лицензионный ключ Сервера администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Перейдите в раздел **Лицензионные ключи** и нажмите на кнопку **Выбрать** в одном из следующих разделов:

   - **Действующая лицензия**, если вы хотите добавить активный лицензионный ключ.
   - **Резервный лицензионный ключ**, если вы хотите добавить резервный лицензионный ключ.

     Вы можете добавить резервный лицензионный ключ только в том случае, если активный лицензионный ключ уже добавлен.

3. В открывшемся окне выберите необходимый лицензионный ключ из таблицы.

   При необходимости вы можете добавить новый лицензионный ключ, нажав на кнопку **Добавить лицензионный ключ** и указав лицензионный ключ в открывшейся правой панели.

4. Нажмите на кнопку **ОК**.

Окно закроется, лицензионный ключ Сервера администрирования добавлен, информация о лицензионном ключе отобразится в разделе **Лицензионные ключи**.

При необходимости вы можете заменить выбранный лицензионный ключ, нажав на кнопку **Изменить** и указав другой лицензионный ключ. Также вы можете удалить лицензионный ключ.

Добавление лицензионного ключа в хранилище Сервера администрирования

При добавлении лицензионного ключа с помощью Kaspersky Security Center Cloud Console 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.

Чтобы добавить лицензионный ключ в хранилище Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии**.

2. Нажмите на кнопку **Добавить**.

3. 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 Cloud 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 **Управление активами** → **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.
6. Выберите устройства, которым будет назначена задача.
7. На шаге мастера **Выбор лицензионного ключа** перейдите по ссылке **Добавить ключ**, чтобы добавить лицензионный ключ.
8. В панели добавления ключа добавьте лицензионный ключ, используя один из следующих параметров:

   Вам необходимо добавить лицензионный ключ только в том случае, если вы не добавляли его в хранилище Сервера администрирования до создания задачи **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.

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.

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.

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 Cloud Console 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** → **Лицензии**.
2. Нажмите на имя лицензионного ключа, который вы хотите автоматически распространять на устройства.
3. В открывшемся окне свойств лицензионного ключа переведите переключатель в положение **Автоматически распространять лицензионный ключ на управляемые устройства**.
4. Нажмите на кнопку **Сохранить**.

Лицензионный ключ будет автоматически распространяться на те устройства, для которых он подходит.

Распространение лицензионного ключа выполняется средствами Агента администрирования. Задачи распространения резервного лицензионного ключа для 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.

Если вы выберите параметр **Автоматически распространять лицензионный ключ на управляемые устройства** для активации любого приложения на управляемом устройстве, и в то же время у вас есть активный лицензионный ключ пробной версии, то ваш лицензионный ключ пробной версии будет автоматически заменен лицензионным ключом подписки за восемь дней до даты истечения срока действия.

Просмотр информации об используемых лицензионных ключах в хранилище Сервера администрирования

Чтобы просмотреть список лицензионных ключей, добавленных в хранилище Сервера администрирования,

В главном окне приложения перейдите в раздел **Операции** → **Лицензии**.

Отобразится список кодов активации, добавленных в хранилище Сервера администрирования.

Чтобы просмотреть подробную информацию о лицензионном ключе:

1. В главном окне приложения перейдите в раздел **Операции** → **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**.

Просмотр информации о лицензионных ключах для выбранного приложения "Лаборатории Касперского"

Чтобы узнать, какие лицензионные ключи используются приложением "Лаборатории Касперского":

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.

   Если устройство принадлежит к группе нераспределенных устройств, перейдите в раздел **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.
2. Нажмите на имя требуемого устройства.
3. В открывшемся окне свойств устройства выберите раздел **Приложения**.
4. В открывшемся списке приложений выберите приложение, лицензионные ключи которой вы хотите просмотреть.
5. В открывшемся окне свойств приложения на вкладке **Общие** выберите раздел **Общие**.

   Информация отображается в рабочей области этого раздела.

Удаление лицензионного ключа Сервера администрирования

Чтобы удалить лицензионный ключ Сервера администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.
2. В открывшемся окне свойств Сервера администрирования выберите раздел **Лицензионные ключи**.
3. Нажмите на кнопку **Удалить активный лицензионный ключ** или **Удалить резервный лицензионный ключ** в зависимости от того, какой лицензионный ключ вы хотите удалить, а затем в открывшемся окне подтвердите операцию.

Лицензионный ключ удален.

Если был добавлен резервный лицензионный ключ, резервный лицензионный ключ автоматически становится активным лицензионным ключом после удаления предыдущего активного лицензионного ключа.

После удаления активного лицензионного ключа Сервера администрирования возможности Системного администрирования и Управления мобильными устройствами становятся недоступными. Можно добавить удаленный лицензионный ключ повторно или добавить другой лицензионный ключ.

Удаление лицензионного ключа из хранилища

Вы можете удалить лицензионный ключ из хранилища Сервера администрирования. Kaspersky Security Center Cloud Console автоматически удаляет вашу рабочую область через 90 дней в следующих случаях:

- Вы удаляете последний лицензионный ключ (активный, резервный или неиспользуемый), добавленный вручную в хранилище.
- Срок действия последнего лицензионного ключа истекает.

Если ваша рабочая область удалена, вы не сможете управлять защитой своей сети с помощью Kaspersky Security Center Cloud Console. Также данные из Kaspersky Security Center Cloud Console будут безвозвратно утеряны. При необходимости можно удалить рабочую область вручную. В противном случае рекомендуется хранить хотя бы один лицензионный ключ в хранилище Сервера администрирования.

Если вы удалили лицензионный ключ, но ранее добавили резервный лицензионный ключ, он автоматически становится активным после удаления предыдущего активного лицензионного ключа или истечения его срока годности.

Если удалить активный лицензионный ключ, который распространен на управляемые устройства, то приложения продолжат работать на управляемых устройствах.

Чтобы удалить лицензионный ключ из хранилища Сервера администрирования:

1. Убедитесь, что Сервер администрирования не использует лицензионный ключ, который вы хотите удалить. Если Сервер администрирования использует такой ключ, вы не сможете удалить ключ. Чтобы выполнить проверку:

   a. Откройте окно свойств 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.

   b. В открывшемся окне свойств Сервера администрирования на вкладке **Общие** выберите раздел **Лицензионные ключи**.

   c. Если в открывшемся разделе отображается требуемый лицензионный ключ, 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 лицензионный ключ не отображается, Сервер администрирования его не использует.

2. В главном окне приложения перейдите в раздел **Операции** → **Лицензии**.

3. Выберите нужный лицензионный ключ и нажмите на кнопку **Удалить**.

4. В появившемся окне установите флажок **Я понимаю риск и хочу удалить лицензионный ключ**. Это означает, что, если вы удаляете последний лицензионный ключ, вы знаете о последующем удалении рабочей области и потере контроля над управляемыми устройствами. Нажмите на кнопку **Удалить**.

В результате выбранный лицензионный ключ удаляется из хранилища.

Можно добавить удаленный лицензионный ключ повторно или добавить другой лицензионный ключ. Если вы удалили последний лицензионный ключ, вы можете добавить лицензионный ключ, пока ваша рабочая область не удалена. Kaspersky Security Center Cloud Console уведомляет администраторов рабочей области за 30 дней, 7 дней и 1 день до удаления.

Просмотр списка устройств, на которых приложение "Лаборатории Касперского" не активировано

Вы можете просмотреть список всех устройств, на которых установлено приложение "Лаборатории Касперского", но не активировано (например, лицензия отсутствует или истек срок действия).

Чтобы просмотреть устройства, на которых не активировано приложение "Лаборатории Касперского":

1. В главном окне приложения перейдите в раздел **Управление активами** → **Задачи**.

   Отобразится список задач.

2. Нажмите на название задачи Обновление, связанной с рассматриваемым приложением "Лаборатории Касперского".

   Окно свойств задачи отображается с несколькими именными вкладками.

3. В окне свойств задачи выберите раздел **Результаты**.

   В столбце **Устройство или подчиненный Сервер** отображаются устройства, на которых задача была выполнена успешно.

4. Сортировать столбец **Устройство или подчиненный Сервер**.

   В столбце **Устройство или подчиненный Сервер** отображаются устройства, на которых задача была выполнена успешно. Устройства, на которых задача не выполнена из-за отсутствия лицензии, являются устройствами, на которых приложение не активировано.

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 и его инсталляционный пакет, прежде чем отзывать Лицензионное соглашение этого приложения. Инсталляционные пакеты необходимо удалить с Сервера администрирования и его виртуальных Серверов администрирования.

Лицензионные соглашения, принятые на виртуальном Сервере администрирования, можно отозвать на виртуальном Сервере администрирования или на главном Сервере администрирования. Лицензионные соглашения, принятые на главном Сервере администрирования, можно отозвать только на главном Сервере администрирования.

Чтобы отозвать Лицензионное соглашение для управляемых приложений "Лаборатории Касперского":

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** окна свойств Сервера администрирования выберите раздел **Лицензионные соглашения**.

   Отобразится список Лицензионных соглашений, принятых при создании инсталляционных пакетов или установке обновлений.

3. В списке выберите Лицензионные соглашения, которые вы хотите отозвать.

   Можно просмотреть следующие свойства Лицензионных соглашений:

   - Дата принятия Лицензионного соглашения.
   - Имя пользователя, принявшего Лицензионное соглашение.
   - Можно ли отозвать Лицензионное соглашение.

4. 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), связанных с Лицензионным соглашением, и их соответствующие имена и типы.

5. В нижней части окна свойств Лицензионного соглашения нажмите на кнопку **Отозвать Лицензионное соглашение**.

   Если выбранное Лицензионное соглашение можно отозвать только путем деинсталляции приложения или если это Лицензионное соглашение можно отозвать только на главном Сервере администрирования, вместо кнопки **Отозвать Лицензионное соглашение** отображается уведомление об этом ограничении.

   > Если существуют какие-либо объекты (инсталляционные пакеты и соответствующие им задачи), которые не позволяют отозвать Лицензионное соглашение, отображается уведомление об этом. 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.

6. 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).

Если срок действия последнего лицензионного ключа истек, Kaspersky Security Center Cloud Console автоматически удалит вашу рабочую область через 90 дней. В результате вы не сможете управлять защитой своей сети с помощью Kaspersky Security Center Cloud Console. Также данные из Kaspersky Security Center Cloud Console будут безвозвратно утеряны. Рекомендуется продлить лицензии, срок действия которых истек, или добавить лицензионные ключи в хранилище Сервера администрирования, чтобы сохранить рабочую область.

Чтобы просмотреть уведомление об истечении срока лицензии:

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Операции** → **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 лицензии срок действия истекает или уже истек.

2. Если вы хотите продлить срок действия лицензии, перейдите по ссылке **Продлить срок действия лицензии** рядом с нужной лицензией.

   Нажимая на ссылку продления срока действия лицензии, вы соглашаетесь передавать в "Лабораторию Касперского" следующие данные: идентификатор программного обеспечения, версию программного обеспечения, локализацию программного обеспечения, идентификатор лицензии и атрибут, который показывает, была ли лицензия предоставлена компанией-партнером. Эти данные необходимы для определения условий продления срока действия лицензии.

3. В открывшемся окне продления срока действия лицензии следуйте инструкциям.

   Срок действия лицензии продлен.

В Kaspersky Security Center Cloud 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 Security Center Cloud Console после истечения срока действия лицензии

После истечения срока действия лицензии "Лаборатория Касперского" может предоставить вам использование Kaspersky Security Center Cloud Console на 90 дней без ограничений. В этот период Сервер администрирования, Агент администрирования и веб-интерфейс Kaspersky Security Center Cloud Console работают без ограничений. Kaspersky Security Center Cloud Console также отправляет статистику KSN в "Лабораторию Касперского" в соответствии с текущими параметрами KSN. Управляемые приложения работают только с ограниченными функциональными возможностями (подробнее см. в документации к соответствующим приложениям).

Когда срок действия лицензии истекает на 90 дней, Kaspersky Security Center Cloud Console автоматически удаляет вашу рабочую область. Если вы хотите сохранить рабочую область, продлите срок действия хотя бы одной лицензии или добавьте ключ в хранилище.

Определения лицензирования

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием приложений "Лаборатории Касперского", управляемых приложением Kaspersky Security Center Cloud Console.

О лицензии

Лицензия – это ограниченное по времени право на использование Kaspersky Security Center Cloud Console, 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 Cloud Console 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 Cloud Console 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.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить лицензионный ключ, активирующий Kaspersky Security Center Cloud Console. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Security Center Cloud Console или после заказа пробной версии Kaspersky Security Center Cloud Console.

Чтобы активировать приложение с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского". Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы.

Если приложение было активировано с помощью кода активации, в некоторых случаях после активации приложение регулярно отправляет запросы на серверы активации "Лаборатории Касперского" для проверки текущего статуса лицензионного ключа. Для отправки запросов необходимо предоставить приложению доступ в интернет.

Если вы потеряли код активации после установки приложения, обратитесь к партнеру "Лаборатории Касперского", у которого вы приобрели лицензию.

Вы не можете использовать файлы ключей для активации управляемых приложений; вы можете применить только коды активации.

О подписке

Подписка на Kaspersky Security Center Cloud Console – это заказ на использование приложения с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку на Kaspersky Security Center Cloud Console 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 Cloud Console 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 Cloud Console по подписке, требуется применить код активации, предоставленный поставщиком услуг.

Вы можете применить другой код активации для использования Kaspersky Security Center Cloud Console 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 Cloud Console.

При использовании приложения по подписке Kaspersky Security Center Cloud Console 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.

Предоставление данных

Пользователь может использовать программное решение Kaspersky Security Center Cloud Console для идентификации и контроля устройств (а также их владельцев), подключенных к программному решению Kaspersky Security Center Cloud Console, при помощи функций управляемых приложений.

Способы предоставления данных:

1. Пользователь вводит данные в интерфейсе Kaspersky Security Center Cloud Console.
2. Агент администрирования получает данные от устройства и передает на Сервер администрирования.
3. Агент администрирования получает данные от управляемого приложения "Лаборатории Касперского" и передает их на Сервер администрирования. Перечень данных, обрабатываемых управляемыми приложениями "Лаборатории Касперского", приведен в справках соответствующих приложений.
4. Данные передаются с подчиненных Серверов администрирования, работающих локально.

Kaspersky Security Center Cloud Console автоматически удаляет рабочую область через 30 дней после истечения срока действия пробной лицензии и через 90 дней после истечения срока действия коммерческой лицензии.

По истечении срока действия лицензии "Лаборатория Касперского" сохраняет данные Пользователя, связанные с алертами и инцидентами, в рабочих областях Пользователя в течение 30 дней.

С действующей лицензией срок хранения алертов и инцидентов составляет 360 дней. По истечении этого периода старые алерты и старые инциденты автоматически удаляются.

Удаление данных, перечисленных в этом разделе, может занять до 24 часов.

Данные, отправленные на серверы "Лаборатории Касперского"

Данные, отправляемые во время активации

При использовании Кода активации для активации ПО, с целью проверки правомерности использования ПО, Пользователь соглашается периодически предоставлять "Лаборатории Касперского" следующую информацию:

- Код активации.
- Уникальный идентификатор активации действующей лицензии.

"Лаборатория Касперского" может также использовать эту информацию для формирования статистической информации о распространении и использовании программного обеспечения "Лаборатории Касперского".

Данные, отправляемые во время обновления

При получении Обновлений с серверов обновления Правообладателя, для целей улучшения качества работы механизма обновления, Пользователь соглашается периодически предоставлять "Лаборатории Касперского" следующую информацию:

- идентификатор ПО, полученный из лицензии;
- полная версия ПО;
- идентификатор лицензии ПО;
- идентификатор установки ПО (PCID);
- идентификатор запуска обновления ПО.

"Лаборатория Касперского" может также использовать эту информацию для формирования статистической информации о распространении и использовании программного обеспечения "Лаборатории Касперского".

Данные для обеспечения бесперебойной, эффективной работы и проверки правомерного использования Kaspersky Security Center Cloud Console

Для указанной цели может быть использована следующая информация:

- Названия и версии приложений безопасности "Лаборатории Касперского", подключенных к рабочей области, и устройства, на которых эти приложения безопасности установлены.
- Количество устройств с установленными приложениями безопасности "Лаборатории Касперского", подключенных к рабочим областям и распределение этих подключенных устройств по типу.
- Идентификатор рабочей области, страна и регион рабочей области и дата создания рабочей области.
- Количество пользователей в рабочей области, дата последней аутентификации в рабочей области.
- Информация об используемой лицензии (тип лицензии, лицензионное ограничение на количество устройств, количество подключенных устройств, дата окончания срока действия использованной ранее лицензии).

Данные, передаваемые при переходе по ссылкам в интерфейсе Kaspersky Security Center Cloud Console

Переходя по ссылкам в Консоли администрирования или Kaspersky Security Center Cloud Console, Пользователь соглашается на автоматическую передачу следующих данных:

- локализация приложения Kaspersky Security Center Cloud Console;
- идентификатор лицензии;
- была ли приобретена лицензия через партнера.

Список данных, предоставляемых по каждой ссылке, зависит от цели и местоположения ссылки.

Данные, необходимые для работы управляемых приложений

Следующие управляемые приложения передают данные с устройства на Сервер администрирования через Агент администрирования:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Mac
- Kaspersky Endpoint Agent
- Kaspersky Endpoint Security для Android
- Kaspersky Security для iOS
- Kaspersky Secure Mobility Management
- Kaspersky Embedded Systems Security для Windows
- Kaspersky Embedded Systems Security для Linux

Список обрабатываемых данных публикуется в Соглашении об обработке данных для Kaspersky при подключении устройств.

Данные Пользователя, обрабатываемые локально

Единственным компонентом Kaspersky Security Center, который может быть развернут локально в Kaspersky Security Center Cloud Console, является Агент администрирования.

Перечень данных Пользователя, обрабатываемых локально:

- Все данные, перечисленные в разделе Данные Пользователя, обрабатываемые в рамках инфраструктуры и систем "Лаборатории Касперского", кроме данных, которые администратор вводит посредством интерфейса Kaspersky Security Center Cloud Console.
- Журнал событий Kaspersky Event Log Агента администрирования.
- Трассировки Агента администрирования.
- Журналы, включая журналы, создаваемые инсталлятором Агента администрирования, утилитами Kaspersky Security Center.

Файлы дампа, журналы, трассировки Агента администрирования содержат случайные данные и могут содержать персональные данные. Файлы хранятся в незашифрованном виде на устройстве, на котором установлен Агент администрирования. Файлы не передаются в "Лабораторию Касперского" автоматически. Пользователь может передать эти данные в "Лабораторию Касперского" вручную по запросу Службы технической поддержки для решения проблем в работе Kaspersky Security Center.

О юридических документах Kaspersky Security Center Cloud Console

Для использования Kaspersky Security Center Cloud Console вам нужно прочитать и согласиться с условиями юридических документов, указанных на веб-сайте Kaspersky Security Center Cloud Console. Вы можете ознакомиться с положениями и условиями Политики конфиденциальности "Лаборатория Касперского" для веб-сайтов при входе в Kaspersky Security Center Cloud Console для управления рабочей областью. Вы можете прочитать Соглашение приложения Kaspersky Security Center Cloud Console и Соглашение приложения Kaspersky Security Center Cloud Console об обработке данных при создании рабочей области организации.

Внимательно прочитайте все юридические документы, прежде чем начать использовать Kaspersky Security Center Cloud Console.

Лицензионное соглашение для приложений "Лаборатории Касперского"

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

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- В окне, которое отображается при создании инсталляционного пакета приложения "Лаборатории Касперского".
- В файле license.txt, в папке установки приложения "Лаборатории Касперского" на управляемом устройстве.

Вы можете отозвать принятое Лицензионное соглашение в любое время.

Если вы не согласны с условиями Лицензионного соглашения приложения "Лаборатории Касперского", вы не можете использовать приложение.

Руководство по усилению защиты

Kaspersky Security Center Cloud Console – это приложение, которое размещается и поддерживается "Лабораторией Касперского". Вам не нужно устанавливать Kaspersky Security Center Cloud Console на свой компьютер или сервер. Kaspersky Security Center Cloud Console позволяет администратору устанавливать приложения безопасности "Лаборатории Касперского" на устройства в корпоративной сети, удаленно запускать задачи проверки и обновления, а также управлять политиками безопасности управляемых приложений.

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

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

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

Руководство по усилению защиты содержит следующую информацию:

- настройка учетных записей для работы с Kaspersky Security Center Cloud Console;
- управление защитой клиентских устройств;
- настройка защиты управляемых приложений;
- передача информации в сторонние системы.

Перед началом работы с Kaspersky Security Center Cloud Console вам будет предложено ознакомиться с краткой версией Руководства по усилению защиты.

Обратите внимание, что вы не можете использовать Kaspersky Security Center Cloud Console, пока не подтвердите, что ознакомились с Руководством по усилению защиты.

Чтобы прочитать Руководство по усилению защиты:

1. Откройте Kaspersky Security Center Cloud Console и выполните вход. Kaspersky Security Center Cloud Console проверяет, подтвердили ли вы, что прочитали текущую версию Руководства по усилению защиты.

   Если вы еще не читали Руководство по усилению защиты, откроется окно с его краткой версией.

2. Выполните одно из следующих действий:

   - Если вы хотите просмотреть краткую версию Руководства по усилению защиты в виде текстового документа, перейдите по ссылке **Открыть в новом окне**.

   - Если вы хотите просмотреть полную версию Руководства по усилению защиты, перейдите по ссылке **Открыть Руководство по усилению защиты в онлайн-справке**.

3. После прочтения Руководства по усилению защиты установите флажок **Я подтверждаю, что полностью прочитал(а) и понимаю Руководство по усилению защиты** и нажмите на кнопку **Принять**.

Теперь можно работать с Kaspersky Security Center Cloud Console.

При появлении новой версии Руководства по усилению защиты Kaspersky Security Center Cloud Console предложит вам ее прочитать.

Планирование архитектуры Kaspersky Security Center Cloud Console

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 Cloud Console и их взаимодействием между собой, а также со схемами трафика данных и использования портов.

На основании этой информации нужно сформировать архитектуру, определяющую:

- организацию рабочих мест администраторов и способы подключения к Kaspersky Security Center Cloud Console;
- 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.

Учетные записи и авторизация

Использование двухфакторной аутентификации Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console предоставляет пользователям возможность двухфакторной аутентификации.

Двухфакторная аутентификация позволяет повысить безопасность вашей учетной записи Kaspersky Security Center Cloud Console. Когда эта функция включена, каждый раз при входе в Kaspersky Security Center Cloud Console с помощью адреса электронной почты и пароля, вы вводите дополнительный одноразовый код безопасности. Вы можете получить одноразовый код безопасности по SMS или сгенерировать его в приложении для аутентификации (в зависимости от параметров двухфакторной аутентификации).

Категорически не рекомендуется устанавливать приложение для аутентификации на устройстве, с которого выполняется подключение к Kaspersky Security Center Cloud Console. Например, вы можете установить приложение для аутентификации на мобильном устройстве.

Запрет на сохранение пароля администратора

При работе с Kaspersky Security Center Cloud Console **категорически не рекомендуется** сохранять пароль администратора в браузере на устройстве пользователя.

Если браузер скомпрометирован, злоумышленник может получить доступ к сохраненным паролям. Также если устройство пользователя с сохраненными паролями украдено или потеряно, злоумышленник может получить доступ к защищенным данным.

Ограничить членство в роли "Главный администратор"

Рекомендуется ограничить членство пользователей в роли "Главный администратор".

При создании рабочей области пользователю по умолчанию присвоена роль Главный администратор. Это удобно для управления, но критично с точки зрения безопасности, так как роль "Главный администратор" имеет очень широкий набор привилегий. Назначение этой роли пользователям должно быть строго регламентировано.

Для организации администрирования Kaspersky Security Center Cloud Console рекомендуется обратить внимание на существующие роли для определенных должностей с заранее настроенным набором прав.

Настройка прав доступа к функциям приложения

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

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 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.

управление защитой клиентских устройств;

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.
- Выполняет роль прокси-сервера KSN для клиентских устройств.

С учетом доступных возможностей рекомендуется защитить устройства, выполняющие роль точек распространения, от несанкционированного доступа любого типа (включая физический доступ).

Настройка защиты управляемых приложений

Настройка защиты сети

Убедитесь, что вы успешно выполнили Сценарий первоначальной настройки Kaspersky Security Center Cloud Console. Этот сценарий также предусматривает выполнение шагов мастера первоначальной настройки.

При работе мастера первоначальной настройки создаются политики и задачи с параметрами по умолчанию. В вашей организации эти параметры могут оказаться не оптимальными или даже запрещенными. Поэтому рекомендуется настроить эти политики и задачи и создать дополнительные политики и задачи, если это необходимо для вашей корпоративной сети.

Установка пароля на выключение защиты и удаление приложения

Чтобы злоумышленники не могли отключить приложения безопасности "Лаборатории Касперского", рекомендуется установить пароль для выключения защиты и удаления приложений безопасности "Лаборатории Касперского". Вы можете установить пароль, например, для Kaspersky Endpoint Security для Windows, Агента администрирования и других приложений "Лаборатории Касперского". После включения защиты паролем рекомендуется заблокировать эти параметры, закрыв их "замком".

Указание пароля для запуска утилиты klmover и деинсталляции Агента администрирования

Настоятельно рекомендуется включить защиту паролем для запуска утилиты klmover и деинсталляции Агента администрирования. Чтобы включить защиту паролем, в параметрах политики Агента администрирования выберите параметр **Использовать пароль деинсталляции**.

При включении параметра **Использовать пароль деинсталляции** также включается защита паролем средствами Cleaner (cleaner.exe).

> Утилита klmover используется только для перемещения управляемых устройств под управление виртуального Сервера администрирования. При установке на управляемое устройство Агента администрирования утилита klmover автоматически копируется в папку установки Агента администрирования.

Использование Kaspersky Security Network

Во всех политиках управляемых приложений и в свойствах Kaspersky Security Center Cloud Console рекомендуется использовать Kaspersky Security Network (KSN) и принять актуальное Положение о KSN. При обновлении Kaspersky Security Center Cloud Console вы также можете принять обновленное Положение о KSN.

Обнаружение новых устройств

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

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

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

Для своевременного реагирования на возникновение нештатных ситуаций рекомендуется настроить отправку Kaspersky Security Center Cloud Console 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 или платформ виртуализации, поддерживаемых 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 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

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 использованию приложений безопасности "Лаборатории Касперского"

Использование пароля KLAdmin в Kaspersky Endpoint Security для Windows

Устройством с установленным приложением Kaspersky Endpoint Security для Windows могут пользоваться несколько пользователей с разным уровнем компьютерной грамотности. Если у пользователей есть неограниченный доступ к приложению Kaspersky Endpoint Security для Windows и его параметрам, общий уровень защиты устройства может быть снижен. Защита паролем позволяет ограничить доступ пользователей к Kaspersky Endpoint Security для Windows в соответствии с предоставленными им правами (например, разрешение на завершение работы приложения).

Один из способов ограничить доступ к приложению Kaspersky Endpoint Security для Windows и его параметрам – это использовать учетную запись KLAdmin. 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. 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.

Соблюдайте следующие рекомендации для защиты организации от кражи пароля KLAdmins:

- **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.

Обнаружение и реагирование на киберугрозы

Для эффективной защиты ИТ-инфраструктуры организации от сложных киберугроз, а также для автоматического обнаружения и анализа инцидентов безопасности рекомендуется использовать функции обнаружения и реагирования следующих решений "Лаборатории Касперского", которые можно интегрировать в интерфейс Kaspersky Security Center Cloud Console:

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

Интерфейс Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console управляется с помощью веб-интерфейса.

Окно приложения 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. Нажмите на имя Сервера администрирования, чтобы открыть свойства Сервера администрирования.
- --**Навигация консоли**. Отображает карту главного меню. Большинство отображаемых разделов можно добавить в закладки или установить в качестве домашней страницы. По умолчанию раздел **Навигация консоли** установлен как домашняя страница. Вы можете изменить эти параметры.
- **Мониторинг**. Предоставляет сведения об инфраструктуре вашей сети, статусе защиты, а также статистику.
- **Управление активами**. Содержит инструменты для управления клиентскими устройствами, а также задачи и политики приложений "Лаборатории Касперского".
- **Пользователи и роли**. Позволяет управлять пользователями и ролями, настраивать права пользователей, назначать пользователям роли и связывать профили политик с ролями.
- **Операции**. Содержит множество операций, включая лицензирование приложений, управление патчами и управление приложениями сторонних производителей. Раздел также предоставляет вам доступ к хранилищам приложений.
- **Обнаружение устройств и развертывание**. Позволяет опрашивать сеть для обнаружения клиентских устройств и распределять устройства по группам администрирования вручную или автоматически. Также 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**. Содержит параметры для интеграции Kaspersky Security Center Cloud Console с другими приложениями "Лаборатории Касперского". Также 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 Cloud Console.

В центре панели находится раскрывающийся список с названием вашей текущей рабочей области. С помощью раскрывающегося списка можно выполнить одно из следующих действий:

- Переключиться на другую рабочую область, если она доступна.
- Вернуться к списку рабочих областей.

В правой части панели отображается меню вашей учетной записи. Вы можете открыть меню, нажав на имя своей учетной записи, и выполнить одно из следующих действий, выбрав соответствующий пункт в раскрывающемся списке:

- Настроить параметры своей учетной записи.

  Если вы выберете пункт **Управление учетной записью**, вы будете перенаправлены на портал Kaspersky Account, где можно сменить пароль или адрес электронной почты, а также настроить двухэтапную аутентификацию.

- Выбрать язык интерфейса Kaspersky Security Center Cloud Console.
- Выбрать светлую тему интерфейса.
- Просмотреть информацию о Службе технической поддержки "Лаборатории Касперского".
- Перейти в справку Kaspersky Security Center Cloud Console.
- Просмотреть обучающие видеоролики о настройке и использовании Kaspersky Security Center Cloud Console и приложений безопасности.

  В браузере Mozilla Firefox, если вы воспроизводите видео в разделе **Обучающие материалы** во всплывающем окне, затем открываете видео в режиме картинка в картинке и закрываете видео во всплывающем окне, видео в режиме картинка в картинке также закрывается.

- Просмотреть информацию о доступных вам юридических документах для приложений "Лаборатории Касперского".
- Выйти из Kaspersky Security Center Cloud Console.

Рабочая область

В рабочей области отображается выбранная вами информация для просмотра в разделах окон веб-интерфейса приложения. Она также содержит элементы управления, которые можно использовать для настройки отображения информации.

Изменение языка интерфейса Kaspersky Security Center Cloud Console

Вы можете выбрать один из поддерживаемых языков локализации в качестве языка интерфейса Kaspersky Security Center Cloud Console.

Чтобы изменить язык интерфейса:

1. В главном окне приложения перейдите в раздел **Параметры** → **Язык**.
2. Выберите необходимый язык интерфейса.

Изменение домашней страницы Kaspersky Security Center Cloud Console

Домашняя страница отображается после входа в Kaspersky Security Center Cloud Console.

По умолчанию вкладка **Параметры домашней страницы** раздела **Навигация консоли** установлена 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.

Закрепление и отмена закрепления разделов главного меню

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

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

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

Чтобы закрепить раздел:

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

   Отображается значок булавки (📌).

2. Нажмите на значок булавки (📌).

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

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

Чтобы отменить закрепление раздела:

1. В главном окне приложения перейдите в раздел **Закладки**.

2. Наведите курсор мыши на раздел, для которого вы хотите отменить закрепление и нажмите на значок отмены закрепления (📌).

   Раздел удален из избранных.

Возврат к списку рабочих областей

После открытия рабочей области вы можете вернуться на страницу портала, на которой отображаются созданные вами рабочие области. Если администраторы других рабочих областей предоставили вам доступ, назначив вашей учетной записи роль гостя или администратора, эти рабочие области также появятся на странице портала.

Чтобы вернуться к списку рабочих областей:

1. На верхней панели нажмите на раскрывающийся список с названием текущей рабочей области.

2. Выберите **Перейти на портал**.

   На странице портала отображается список рабочих областей.

Первоначальная конфигурация Kaspersky Security Center Cloud Console

В этом разделе описаны принципы основного сценария развертывания Kaspersky Security Center Cloud Console, которое начинается с создания рабочей области и заканчивается контролем состояния системы защиты.

Информация о развертывании приложения Kaspersky Security Center для работы локально приведена в справке Kaspersky Security Center.

Рекомендуется отвести на выполнение этого сценария не менее одного рабочего дня.

Сценарий позволяет выполнить следующее:

- Начать работать с рабочей областью в качестве администратора.
- Обнаруживать устройства в своей сети (при необходимости вы будете назначать точки распространения и вручную устанавливать на них дистрибутивы).
- Разворачивать управляемые приложения "Лаборатории Касперского" на клиентских устройствах и настраивать инструменты для защиты сети, мониторинга и регулярного обновления баз, модулей приложений и приложений "Лаборатории Касперского".

После завершения этого сценария будет настроена защита сети на основе приложений "Лаборатории Касперского". В сможете приступить к контролю состояния защиты сети.

Предварительные требования

Прежде чем начать:

- Ознакомьтесь с архитектурой Kaspersky Security Center Cloud Console, чтобы понять взаимодействие между основными компонентами приложения.
- Прочтите информацию о лицензировании Kaspersky Security Center Cloud Console и управляемых приложениях.
- Убедитесь, что у вас есть действительный код активации для Kaspersky Security Center Cloud Console (если вы создаете коммерческую рабочую область).

Этапы

Конфигурация Kaspersky Security Center Cloud Console происходит поэтапно:

1. **Настройка портов**

   Убедитесь, что все необходимые порты открыты для взаимодействия между вашей сетью и инфраструктурой "Лаборатории Касперского". Также, если вы планируете использовать иерархию Серверов администрирования, убедитесь, что все необходимые порты открыты для взаимодействия между подчиненным Сервером (или подчиненными Серверами) и клиентскими устройствами.

2. **Создание рабочей области**

   Создайте учетную запись, а затем создайте рабочую область.

3. **Выполнение мастера первоначальной настройки**

   Откройте Kaspersky Security Center Cloud Console и зайдите под своей учетной записью. При первом входе вам автоматически предлагается запустить мастер первоначальной настройки. Вы также можете запустить мастер первоначальной настройки вручную в любое время.

   После завершения работы мастера первоначальной настройки у вас будут инсталляционные пакеты Агента администрирования и приложений безопасности. Эти инсталляционные пакеты потребуются для дальнейшего развертывания Kaspersky Security Center Cloud Console.

4. **Развертывание приложений "Лаборатории Касперского"**

   Выполните сценарий первоначального развертывания приложений "Лаборатории Касперского". Один из шагов сценария относится к операции опроса сети. Эта операция необходима для обнаружения клиентских устройств вашей сети. Сетевой опрос и его параметры описаны в сценарии обнаружения сетевых устройств.

5. **Лицензирование приложений безопасности "Лаборатории Касперского"**

   Когда приложения безопасности "Лаборатории Касперского" разворачиваются на управляемых устройствах, они должны быть лицензированы путем применения кода активации для каждого из приложений. Распространите коды активации на приложения "Лаборатории Касперского", установленные на управляемых устройствах. Существует несколько вариантов лицензирования приложений безопасности "Лаборатории Касперского".

6. **Настройка защиты сети**

   Выполните настройку защиты сети, чтобы настроить политики и задачи, созданные с помощью мастера первоначальной настройки. Обратите внимание на оптимизацию нагрузки на приложения для защиты конечных точек.

7. **Регулярное обновление баз, модулей приложений и приложений "Лаборатории Касперского"**

   Чтобы ваша сеть была защищена от вирусов и других угроз, вам необходимо настроить регулярные обновления баз, модулей приложений и приложений "Лаборатории Касперского".

8. **Обновление приложений сторонних производителей и поиск уязвимостей в приложениях сторонних производителей (если требуется)**

   Kaspersky Security Center Cloud Console позволяет управлять обновлениями приложений Microsoft, установленных на клиентских устройствах. Вы также можете закрыть уязвимости в приложениях Microsoft, установив необходимые обновления.

9. **Настройка инструментов для контроля состояния защиты сети**

   Выберите и настройте виджеты, отчеты и другие инструменты, которые позволяют контролировать состояние защиты сети.

После развертывания и настройки Kaspersky Security Center Cloud Console вы можете приступить к контролю состояния защиты сети.

Сценарий: создание иерархии Серверов администрирования, управляемых с помощью Kaspersky Security Center Cloud Console

В этом сценарии описываются действия, которые необходимо выполнить для создания иерархии Серверов администрирования, управляемых с помощью Kaspersky Security Center Cloud Console, которая, таким образом, выполняет роль главного Сервера администрирования. Эта иерархия может впоследствии использоваться для переноса данных управляемых устройств и объектов из приложения Kaspersky Security Center в приложение Kaspersky Security Center Cloud Console, а также для управления подчиненными Серверами администрирования и устройствами с помощью Kaspersky Security Center Cloud Console.

Kaspersky Security Center Cloud Console может выполнять роль только главного Сервера администрирования, а локальные Серверы администрирования могут выполнять роль только подчиненных Серверов администрирования. Другие схемы иерархии недоступны.

Предварительные требования

Убедитесь, что выполнены следующие предварительные требования:

- Обновление Сервера администрирования, работающего локально, до версии 12 или выше.
- Установка Kaspersky Security Center Web Console на Сервера администрирования, работающего локально.
- Установка веб-плагинов для приложений, которыми вы планируете управлять с помощью Kaspersky Security Center Cloud Console.
- Обновление управляемых приложений до версий, поддерживаемых Kaspersky Security Center Cloud Console.
- Убедитесь, что в задаче Загрузка обновлений в хранилище Сервера администрирования на локальном Сервере администрирования главный Сервер администрирования не назначен в качестве источника обновлений. Измените параметры задачи, если это необходимо.

После того, как создана иерархия политики и задачи, которые действуют в Kaspersky Security Center Cloud Console, применяются на подчиненном Сервере администрирования, заменяя существующие политики и задачи. Чтобы избежать такой ситуации, удалите все политики и задачи Kaspersky Security Center Cloud Console перед созданием иерархии. Также вы можете изменить состояние каждой политики Kaspersky Security Center Cloud Console на **Неактивна** в ее параметрах и выключить параметр **Распространить на подчиненные и виртуальные Серверы администрирования** в свойствах каждой задачи Kaspersky Security Center Cloud Console.

Вы можете удалить иерархию Серверов администрирования в любое время, если это необходимо.

Этапы создания иерархии

Основной сценарий предусматривает подчиненный Сервер администрирования, к которому невозможно получить доступ из интернета. Однако набор действий некоторых из описанных ниже шагов может отличаться, если подчиненный Сервер администрирования доступен из интернета. Также в этом случае некоторые шаги нужно пропустить.

Создание иерархии Серверов администрирования состоит из следующих этапов:

1. **Получение сертификата подчиненного Сервера администрирования**

   Если подчиненный Сервер администрирования доступен из интернета, пропустите этот шаг.

   В приложении Kaspersky Security Center Web Console, работающем локально, откройте свойства Сервера администрирования и на вкладке **Общие** откройте раздел **Общие**. Перейдите по ссылке **Просмотреть сертификат Сервера администрирования**. Файл сертификата в формате CER автоматически сохраняется в папке, указанной в параметрах вашего браузера.

2. **Получение параметров подключения и сертификатов из Kaspersky Security Center Cloud Console**

   Если подчиненный Сервер администрирования доступен из интернета, пропустите этот шаг.

   В приложении Kaspersky Security Center Cloud Console откройте свойства Сервера администрирования на вкладке **Общие** и откройте раздел **Иерархия Серверов администрирования**. Отображаются следующие параметры подключения:

   - **HDS-адрес**

     Отображается веб-адрес, используемый для подключения к Hosted Discovery Service (HDS).

   - **HDS-порт**

     Отображается номер порта, используемого для подключения к HDS.

   Раздел также содержит две ссылки:

   - **Просмотреть сертификат Сервера администрирования**

     При переходе по этой ссылке начинается загрузка открытого ключа экземпляра сертификата Kaspersky Security Center Cloud Console.

   - **HDS-сертификат, выпущенный корневым центром сертификации**

     При переходе по этой ссылке начинается загрузка файла с расширением pem, который содержит список доверенных корневых сертификатов, подписанных аккредитованным Центром сертификации (CA). Этот файл предназначен для использования подчиненным Сервером администрирования: он требуется для проверки HDS-сертификата.

Скопируйте параметры подключения вручную, с помощью буфера обмена или любым другим удобным способом, и сохраните их в файл любого удобного формата. Перейдите по ссылке **Просмотреть сертификат Сервера администрирования** и дождитесь загрузки файла сертификата. Перейдите по ссылке **HDS-сертификат, выпущенный корневым центром сертификации** и дождитесь загрузки файла со списком доверенных корневых сертификатов, подписанных аккредитованным Центром сертификации. Оба файла сохраняются в папке, указанной в параметрах вашего браузера.

3. **Выбор подчиненного Сервера администрирования для подключения**

В свойствах Сервера администрирования перейдите на вкладку **Серверы администрирования**. В иерархии групп администрирования установите флажок рядом с группой администрирования, в которой вы хотите разместить подчиненный Сервер администрирования со всеми его управляемыми устройствами. Нажмите на кнопку **Подключить подчиненный Сервер администрирования**.

На открывшейся странице в поле **Имя подчиненного Сервера администрирования** укажите имя, под которым подчиненный Сервер администрирования должен отображаться в иерархии. Это имя используется только для вашего удобства и поэтому при необходимости может отличаться от реального имени подчиненного Сервера администрирования. Нажмите на кнопку **Далее**.

Если подчиненный Сервер администрирования доступен из интернета, вы также должны указать адрес подчиненного Сервера администрирования в поле **Адрес подчиненного Сервера администрирования (необязательно)**.

На следующей странице нажмите на кнопку **Обзор** и укажите файл с расширением pem, который вы сохранили с подчиненного Сервера администрирования. Нажмите на кнопку **Далее**.

4. **Включение и настройка параметров прокси-сервера**

Действия этого этапа являются необязательными. Выполняйте их, только если в вашем случае соединение требует использование прокси-сервера.

Нажмите на кнопку **Далее**. На странице **Параметры подключения и аутентификации**, вы можете включить и настроить использование прокси-сервера, если это необходимо. Установите флажок **Использовать прокси-сервер** и укажите следующие параметры прокси-сервера:

- **Адрес прокси-сервера**

  Адрес прокси-сервера.

- **Имя пользователя**

  Имя пользователя для входа на прокси-сервер.

- **Пароль**

  Пароль для входа на прокси-сервер.

5. **Задание параметров аутентификации и добавление подчиненного Сервера администрирования в иерархию**

Нажмите на кнопку **Далее**. На странице **Учетные данные подчиненного Сервера администрирования** укажите следующие параметры:

- **Имя пользователя**

  Имя пользователя, под которым вы входите на подчиненный Сервер администрирования.

- **Пароль**

  Пароль, используемый для входа на подчиненный Сервер администрирования.

Нажмите на кнопку **Далее** и дождитесь появления подчиненного Сервера администрирования в иерархии.

Если подчиненный Сервер администрирования доступен из интернета, он подключается к главному Серверу администрирования.

> Если подчиненный Сервер администрирования доступен из интернета и соединение между двумя Серверами администрирования успешно установлено, пропустите все следующие шаги.

Если к подчиненному Серверу администрирования невозможно получить доступ из интернета, он становится видимым, но для получения над ним контроля необходимо выполнить дополнительные действия на подчиненном Сервере администрирования.

6. **Настройка подключения в приложении Kaspersky Security Center Web Console, работающем локально**

   В приложении Kaspersky Security Center Web Console, работающей локально, откройте свойства Сервера администрирования и на вкладке **Общие** откройте раздел **Иерархия Серверов администрирования**. Установите флажок **Этот Сервер администрирования является подчиненным в иерархии**. В списке **Тип главного Сервера администрирования** выберите параметр **Kaspersky Security Center Cloud Console**.

   > Kaspersky Security Center Web Console проверяет, указан ли главный Сервер администрирования в качестве источника обновлений в задаче *Загрузить обновления в хранилище Сервера администрирования*. Если в качестве источника обновлений указан главный Сервер администрирования, вы получите соответствующее сообщение и ссылку на параметры задачи. Вы можете изменить параметры, а затем вернуться к созданию иерархии, или вы можете пропустить это действие и продолжить создание иерархии.

   В группе **Параметры для соединения между подчиненным и главным Серверами администрирования** укажите следующие параметры:

   - **Адрес HDS-сервера (для главного Сервера администрирования на Kaspersky Security Center Cloud Console)**

     Введите адрес HDS-сервера в формате полного доменного имени (FQDN); вы скопировали и сохранили этот адрес из свойств Сервера администрирования в Kaspersky Security Center Cloud Console.

   - **Порты HDS-сервера**

     Введите номера портов HDS-сервера, которые вы скопировали и сохранили из свойств Сервера администрирования в Kaspersky Security Center Cloud Console.

7. **Добавление сертификатов на подчиненный Сервер администрирования**

   Нажмите на кнопку **Укажите сертификат главного Сервера администрирования** и укажите файл сертификата, который вы сохранили в свойствах Сервера администрирования в Kaspersky Security Center Cloud Console.

   Нажмите на кнопку **Укажите сертификат службы Hosted Discovery Service** и укажите файл .pem, который вы сохранили из свойств Сервера администрирования в Kaspersky Security Center Cloud Console.

Если вы включили использование прокси-сервера при подключении подчиненного Сервера администрирования в Kaspersky Security Center Cloud Console, установите флажок **Использовать прокси-сервер** и укажите параметры прокси-сервера, как и в Kaspersky Security Center Cloud Console.

Вы также можете установить флажок **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**, если подчиненный Сервер администрирования находится в демилитаризованной зоне (DMZ).

Подчиненный Сервер администрирования подключается к главному Серверу администрирования.

Результаты

Выполнив вышеуказанные шаги, вы можете убедиться, что иерархия создана успешно:

- Активные политики главного Сервера администрирования вступают в силу на подчиненном Сервере администрирования. Задачи главного Сервера администрирования распространяются на подчиненный Сервер администрирования. Если параметр **Распространить на подчиненные и виртуальные Серверы администрирования** включен в параметрах групповой задачи, каждая такая задача также распространяется на подчиненный Сервер администрирования.
- Параметры политики, заблокированные для изменений на главном Сервере администрирования, отображаются как заблокированные для изменений во всех политиках на подчиненном Сервере администрирования.
- Политики, примененные на главном Сервере администрирования, отображаются в списке политик подчиненного Сервера администрирования (**Управление активами** → **Политики**).
- Групповые задачи, распространенные главным Сервером администрирования, отображаются в списке задач подчиненного Сервера администрирования (**Управление активами** → **Задачи**).
- Политики и задачи, созданные на главном Сервере администрирования, невозможно изменить на подчиненном Сервере администрирования.
- В структуре групп администрирования Kaspersky Security Center Cloud Console подчиненный Сервер администрирования отображается в группе, выбранной вами при добавлении Сервера администрирования.

Перенос данных в Kaspersky Security Center Cloud Console

В этом разделе описывается перенос данных управляемых устройств из приложения Kaspersky Security Center версии 12 и выше, работающего локально, в Kaspersky Security Center Cloud Console.

Перенос данных из Kaspersky Security Center Linux в Kaspersky Security Center Cloud Console не поддерживается.

Способы переноса данных в Kaspersky Security Center Cloud Console

С помощью функции переноса данных вы можете перенести сетевые устройства из Kaspersky Security Center под управление Kaspersky Security Center Cloud Console. Управляемые устройства переключаются без потери основных параметров (например принадлежность к группам администрирования) и основных объектов (например, политик и задач, связанных с управляемыми приложениями).

Вы можете выбрать один из двух доступных способов переноса данных Серверов администрирования в Kaspersky Security Center Cloud Console:

- Перенос данных без иерархии Серверов администрирования:
  - Позволяет передавать управляемые устройства и связанные объекты в Kaspersky Security Center Cloud Console, даже если локальный Сервер администрирования не является подчиненным по отношению к Kaspersky Security Center Cloud Console.
  - Может потребоваться передача файлов (на съемном диске, по электронной почте, с помощью общих папок или любым другим удобным способом), если Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console запущены на разных физических устройствах.

  Вы также можете выполнить перенос данных с виртуальными Серверами администрирования, если они есть в вашей сети.

- Перенос данных с использованием иерархии Серверов администрирования:
  - Позволяет переносить управляемые устройства и связанные объекты в Kaspersky Security Center Cloud Console, используя только интерфейс Kaspersky Security Center Cloud Console, поэтому физическая передача файлов не требуется.
  - Требуется, чтобы Сервер администрирования, работающий локально, выполняющих роль подчиненного Kaspersky Security Center Cloud Console. Вы можете создать такую иерархию перед началом переноса данных.

Для полнодискового шифрования Kaspersky Security Center Cloud Console поддерживает только BitLocker.

Сценарий: перенос данных без иерархии Серверов администрирования

В этом разделе описывается перенос данных управляемых устройств и связанных с ними объектов (таких как политики, задачи, отчеты) из приложения Kaspersky Security Center Web Console, работающего локально, в Kaspersky Security Center Cloud Console. Вы можете включить одну группу администрирования в область переноса данных, чтобы восстановить эту группу администрирования в Kaspersky Security Center Cloud Console.

В эту группу должны входить управляемые устройства одной операционной системы. Если ваша сеть включает устройства с разными операционными системами или дистрибутивами Linux, распределите их по разным группам администрирования, а затем перенесите данные каждой группы отдельно.

После завершения переноса данных все Агенты администрирования, входящие в область переноса данных, обновляются и переходят под управление Kaspersky Security Center Cloud Console.

Шаги, перечисленные в этом разделе, описывают процесс переноса данных, выполняемый при отсутствии иерархии Серверов администрирования, то есть когда соединение между Kaspersky Security Center Cloud Console и приложением Kaspersky Security Center Web Console, работающем локально, не установлено.

Предварительные требования

Прежде чем начать, сделайте следующее:

- Обновите Сервер администрирования, работающий локально, до версии 14.2 или выше.
- Установите приложение Kaspersky Security Center Web Console версии 12.1 или выше.
- Обновите Агент администрирования на управляемых устройствах до версии 12 или выше.
- На устройствах с операционной системой Windows используйте Агент администрирования без пароля для деинсталляции.

  Если пароль уже задан, выполните одно из следующих действий в Kaspersky Security Center Web Console:

  - Выключите параметр **Использовать пароль деинсталляции** в свойствах политики Агента администрирования.
  - Удалите Агент администрирования удаленно с помощью задачи *Удаленная деинсталляция приложения*. В поле задачи **Приложение для деинсталляции** выберите значение **Агент администрирования Kaspersky Security Center**. Введите пароль для деинсталляции.
- Обновите управляемые приложения до версий, поддерживаемых Kaspersky Security Center Cloud Console.
- Убедитесь, что у вас есть политики для последних версий управляемых приложений. Если вы используете устаревшие политики, создайте политики для версий приложений, поддерживаемых Kaspersky Security Center Cloud Console.

- Чтобы использовать действующие политики, обновите веб-плагины для приложений, которыми вы планируете управлять с помощью Kaspersky Security Center Cloud Console.
- Удалите приложения "Лаборатории Касперского" с управляемых устройств, если эти приложения не поддерживаются Kaspersky Security Center Cloud Console.
- Расшифруйте все данные (на уровне диска или на уровне файлов), зашифрованные Kaspersky Endpoint Security для Windows на управляемых устройствах под управлением операционной системы Windows, и выключите функцию шифрования на управляемых устройствах с помощью политики приложения или локально. Дополнительную информацию см. в справке Kaspersky Endpoint Security для Windows.

  Если на устройстве с операционной системой Windows все еще хранятся какие-либо файлы или папки, зашифрованные с помощью Kaspersky Endpoint Security для Windows, обновление Агента администрирования будет отменено во время процесса переноса данных. Уведомление предложит вам расшифровать все данные на устройстве и отключить функцию шифрования.

Максимальное количество управляемых устройств на один Сервер администрирования в Kaspersky Security Center Cloud Console равно 25 000.

Этапы переноса данных

Перенос данных в Kaspersky Security Center Cloud Console включает в себя следующие этапы:

1. **Планирование области переноса данных и проверка предварительных требований**

   Оцените область переноса данных, то есть просмотрите группу администрирования для экспорта, и оцените количество управляемых устройств в ней. Также убедитесь, что все действия, перечисленные в качестве предварительных требований переноса данных, были успешно выполнены.

2. **Экспорт управляемых устройств, объектов и параметров из Kaspersky Security Center Web Console**

   Используйте мастер переноса данных приложения Kaspersky Security Center Web Console, работающего локально, для экспорта управляемых устройств вместе с их объектами.

   Максимальный размер файла экспорта составляет 4 ГБ.

3. **Импорт файла экспорта в Kaspersky Security Center Cloud Console**

   Перенесите информацию об управляемых устройствах и объектах в приложение Kaspersky Security Center Cloud Console. Для этого используйте мастер переноса данных Kaspersky Security Center Cloud Console, чтобы импортировать файл экспорта и создать автономный инсталляционный пакет Агента администрирования.

4. **Переустановка Агента администрирования на управляемых устройствах**

   Вернитесь в мастер переноса данных в экземпляре Kaspersky Security Center Web Console, работающего локально, чтобы создать задачу удаленной установки. Вы сможете использовать эту задачу (сразу или позже) для переустановки Агента администрирования на свои управляемые устройства и завершения процесса переноса данных.

Результаты

После завершения переноса данных вы можете убедиться, что перенос данных прошел успешно:

- Агент администрирования перестановлен на всех управляемых устройствах.
- Все устройства управляются через Kaspersky Security Center Cloud Console.
- Все параметры объектов, действовавшие до переноса данных, сохранились.

Мастер переноса данных

В этом разделе представлена информация о мастере переноса данных в Kaspersky Security Center Cloud Console и Kaspersky Security Center Web Console версии 12 и выше.

Шаг 1. Экспорт управляемых устройств, объектов и параметров из Kaspersky Security Center Web Console

Для переноса данных управляемых устройств из Kaspersky Security Center Web Console в Kaspersky Security Center Cloud Console необходимо сначала создать файл экспорта, содержащий информацию об иерархии групп администрирования на вашем текущем Сервере администрирования, работающем локально. Файл экспорта должен также содержать информацию об объектах и их параметрах. Файл экспорта будет использоваться для последующего импорта в Kaspersky Security Center Cloud Console.

Максимальный размер файла экспорта составляет 4 ГБ.

Чтобы экспортировать объекты и их параметры из Kaspersky Security Center Web Console:

1. В главном меню Kaspersky Security Center Web Console перейдите в раздел **Операции** → **Перенос данных**.
2. На странице приветствия мастера переноса данных нажмите на кнопку **Далее** Откроется страница **Управляемые устройства для экспорта**, на которой отображается вся иерархия групп администрирования соответствующего Сервера администрирования.
3. На странице **Управляемые устройства для экспорта** нажмите на значок шеврона (›) рядом с группой **Управляемые устройства**, чтобы раскрыть иерархию групп администрирования. Выберите группу администрирования, которую вы хотите экспортировать.

   После переноса данных из приложения Kaspersky Security Center, работающего локально, в Kaspersky Security Center Cloud Console, выполненного для двух групп администрирования, задачи удаленной установки для этих групп отображаются с одинаковыми именами.

4. Выберите управляемые приложения, политики и задачи, которые необходимо перенести в Kaspersky Security Center Cloud Console вместе с объектами группы администрирования. Чтобы выбрать управляемые приложения, чьи объекты необходимо экспортировать, установите флажки рядом с их именами в списке.

   Несмотря на то, что Сервер администрирования Kaspersky Security Center есть в списке, установка соответствующего флажка не приводит к экспорту политик Сервера администрирования.

   Чтобы убедиться, что управляемые приложения поддерживаются Kaspersky Security Center Cloud Console, перейдите по соответствующей ссылке. Ссылка перенаправит вас в раздел справки, содержащий список приложений, управляемых Kaspersky Security Center Cloud Console.

   > Если вы выберете приложения, которые не поддерживаются приложением Kaspersky Security Center Cloud Console, политики и задачи этих приложений будут экспортированы, а затем импортированы, но вы не сможете управлять ими в Kaspersky Security Center Cloud Console из-за недоступности плагинов.

5. Просмотрите список групповых объектов, экспортируемых по умолчанию, и укажите объекты, не относящиеся к группе, которые нужно экспортировать вместе с выбранной группой администрирования, если это необходимо. Настройте область экспорта, включив или исключив различные объекты, такие как глобальные задачи, пользовательские выборки устройств, отчеты, пользовательские роли, внутренние пользователи и группы безопасности, а также пользовательские категории программ. Эта страница содержит следующие разделы:

   - **Глобальные задачи**

     Список глобальных задач управляемых приложений, а также глобальных задач Агента администрирования.

     > Если выбранная вами глобальная задача применяется к определенной выборке объектов, эта выборка также будет экспортирована.

     > Несмотря на то, что глобальные задачи Сервера администрирования есть в списке, вы не можете их экспортировать; выбор этих задач не влияет на область экспорта. Задачи удаленной установки также не входят в область экспорта, так как соответствующие инсталляционные пакеты невозможно экспортировать.

   - **Выборки устройств**

     Список пользовательских выборок устройств.

   - **Reports**

     Редактируемый список отчетов для экспорта.

     > Если выбранный вами отчет применяется к определенной выборке объектов, эта выборка также будет экспортирована.

     > Kaspersky Security Center Cloud Console содержит такой же набор шаблонов отчетов, как и Kaspersky Security Center Web Console, поэтому вы можете выбрать для экспорта только те отчеты, которые вы создали вручную или перенастроили.

- **Групповые объекты**

  Список групповых объектов для экспорта по умолчанию. Следующие объекты, связанные с выбранной группой администрирования, будут экспортированы полностью по умолчанию:

  - Структура группы администрирования, то есть все вложенные группы выбранной группы администрирования.
  - Устройства, которые были включены в группы администрирования для экспорта.
  - Теги, назначенные экспортируемым устройствам.

    Если тег был создан в Kaspersky Security Center Web Console, но никогда не был назначен никакому устройству, он не будет экспортирован. Также правила автоматического назначения тегов не будут экспортированы.

  - Групповые политики выбранных управляемых приложений.

    Политики Сервера администрирования и политики Агента администрирования не экспортируются.

  - Групповые задачи выбранных управляемых приложений и групповые задачи Агента администрирования.

    Задачи Сервера администрирования не экспортируются.

  Вы также можете запретить экспорт определенных типов объектов, не относящихся к группе:

  - Чтобы отменить экспорт пользовательских ролей (то есть созданных только пользователем), установите флажок **Исключить пользовательские роли из экспорта**.
  - Чтобы отменить экспорт для внутренних пользователей и групп безопасности, установите флажок **Исключить пользовательские роли и внутренние группы безопасности из экспорта**.
  - Чтобы отменить экспорт пользовательских категорий приложений, пополняемых вручную, установите флажок **Исключить пользовательские категории приложений из экспорта**.

Если вы переносите устройства с различными операционными системами в Kaspersky Security Center Cloud Console, объекты, не относящиеся к группе, необходимо перенести только один раз.

Мастер переноса данных выполняет проверку общего количества управляемых устройств, включенных в выбранную группу администрирования. Если это количество превышает 10 000, появится сообщение об ошибке. Кнопка **Далее** остается неактивной до тех пор, пока количество управляемых устройств в выбранной группе администрирования будет меньше максимально допустимого значения.

6. После того как вы определили область переноса данных, нажмите на кнопку **Далее**, чтобы начать процесс экспорта. Откроется страница **Создание экспортного файла**, на которой можно просмотреть выполнение экспорта для каждого типа объектов, включенных в область переноса данных. Дождитесь, пока значки (🔄) рядом со всеми пунктами в списке объектов заменятся на зеленые флажки (✓). После того как экспорт заканчивается, файл экспорта автоматически загружается в папку загрузки, определенную в параметрах вашего браузера по умолчанию. Имя файла экспорта отображается в нижней части окна браузера.

7. После отображения страницы **Экспорт успешно завершен**, перейдите к следующему этапу, выполняемому в Kaspersky Security Center Cloud Console.

Если вы используете Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console на разных устройствах, необходимо скопировать файл экспорта на съемный диск или выбрать другие способы передачи файла.

Шаг 2. Импорт файла экспорта в Kaspersky Security Center Cloud Console

Чтобы передать информацию об управляемых устройствах, объектах и их параметрах, которые вы экспортировали из Kaspersky Security Center Web Console, вам нужно импортировать ее в приложение Kaspersky Security Center Cloud Console, развернутую в вашей рабочей области. Это позволит вам создать автономный инсталляционный пакет и использовать его для переустановки Агента администрирования на ваших управляемых устройствах.

Перед чем запустить мастер переноса данных в Kaspersky Security Center Cloud Console, убедитесь, что в процессе экспорта текущий язык локализации совпадает с языком локализации Kaspersky Security Center Web Console. При необходимости измените язык локализации.

Если вы ранее завершили мастер первоначальной настройки в рабочей области Kaspersky Security Center Cloud Console, то группа **Управляемые устройства** включает политики и задачи, созданные с параметрами по умолчанию. Удалите эти политики и задачи перед импортом тех, которые вы экспортировали из Kaspersky Security Center Web Console.

Чтобы импортировать файл экспорта в Kaspersky Security Center Cloud Console:

1. В главном меню Kaspersky Security Center Cloud Console, перейдите в раздел **Операции → Перенос данных**.

2. На странице приветствия мастера переноса данных нажмите на кнопку **Импортировать**. В открывшемся окне проводника выберите файл экспорта, перейдя в папку, в которой он был сохранен, и нажмите на кнопку **Открыть**. Дождитесь пока значок (🔄) рядом с файлом статуса загрузки изменится на зеленый флажок (✓).

3. Нажмите на кнопку **Далее**. Откроется следующая страница, на которой отображается вся иерархия групп администрирования Сервера администрирования в Kaspersky Security Center Cloud Console.

4. Установите флажок рядом с целевой группой администрирования, в которую должны быть восстановлены объекты группы, и нажмите на кнопку **Далее**. Мастер переноса данных отображает список инсталляционных пакетов Агента администрирования, доступных в Kaspersky Security Center Cloud Console.

5. Выберите инсталляционный пакет, содержащий соответствующую версию и локализацию Агента администрирования, и нажмите на кнопку **Далее**.

   Выберите инсталляционный пакет Агента администрирования для Windows, только если вы предварительно завершили мастер первоначальной настройки в рабочей области Kaspersky Security Center Cloud Console и если вы выполнили перенос данных для устройств под управлением операционной системы Windows.

   Подождите, пока мастер переноса данных создаст автономный инсталляционный пакет. Максимальный размер файла автономного инсталляционного пакета для Агента администрирования составляет 200 МБ.

   Файл распаковывается и автоматически загружается в папку загрузки, определенную в параметрах вашего браузера по умолчанию. Объекты, не относящиеся к группе, и объекты группы восстанавливаются в целевой группе администрирования.

   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 вы импортировали всю группу **Управляемые устройства**, рекомендуется переименовать только что импортированную подгруппу, чтобы избежать путаницы:

   a. Перейти в раздел **Иерархия групп**.

   b. Нажмите на имя подгруппы в дереве групп.

   c. В открывшемся окне свойств в поле **Имя** введите другое имя (например, "Перенесенные устройства").

   Рекомендуется проверить, успешно ли импортированы объекты (политики, задачи и управляемые устройства), входящие в область экспорта, в Kaspersky Security Center Cloud Console. Для этого перейдите в раздел **Управление активами** и проверьте, появились ли импортированные объекты в списках **Политики** и **Задачи**, а также в подразделах **Активы (Устройства)**.

   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. После этого устройства начинают переключаться на Kaspersky Security Center Cloud Console.

6. Нажмите на кнопку **Готово**, чтобы завершить работу мастера переноса данных.

7. Если вы хотите найти и снова загрузить автономный инсталляционный пакет, перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты** и нажмите на кнопку **Просмотреть список автономных пакетов**. В открывшемся списке выберите созданный вами автономный инсталляционный пакет и нажмите на кнопку **Скачать**.

   Если вы используете Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console на разных устройствах, вам нужно скопировать автономный инсталляционный пакет на съемный диск или выбрать другие способы передачи файла.

Шаг 3. Переустановка Агента администрирования на управляемых устройствах с помощью Kaspersky Security Center Cloud Console

После создания автономного инсталляционного пакета Агента администрирования вы можете приступить к созданию задачи удаленной установки. Выполнение этой задачи позволяет вам переустановить Агент администрирования на всех управляемых устройствах, чтобы эти устройства переключались под управление с помощью Kaspersky Security Center Cloud Console.

Чтобы снизить риск потери данных, рекомендуется сначала выполнить действия для небольшой группы администрирования, насчитывающей до 20 управляемых устройств (не включающих физических серверов), расположенных в корпоративной сети. После завершения этих действий проверьте, успешно ли завершилась повторная установка, и перейдите к повторной установке в полном объеме.

Чтобы создать задачу удаленной установки и переустановить Агент администрирования:

1. Вернитесь в мастер переноса данных в экземпляре Kaspersky Security Center Web Console, работающего локально.

   Рекомендуется использовать мастер переноса данных для создания задачи удаленной установки для переустановки Агента администрирования, как описано ниже. Если необходимо использовать пользовательскую задачу удаленной установки, требуется предварительно вручную создать пользовательский инсталляционный пакет из автономного инсталляционного пакета Агента администрирования. Обратите внимание, что при создании пользовательского инсталляционного пакета вам нужно указать ключ "-s" в командной строке исполняемого файла. Иначе переустановка Агента администрирования из этого пользовательского инсталляционного пакета завершится с ошибкой.

   В зависимости от текущего состояния мастера переноса данных вы можете выполнить одно из следующих действий:

   - Если вы не закрыли мастер переноса данных после экспорта и сеанс еще не истек, нажмите на кнопку **Вернуться к шагу 3 мастера переноса данных**. Установите флажок **Загрузить автономный инсталляционный пакет** и нажмите на кнопку **Выберите автономный инсталляционный пакет**. В открывшемся окне браузера укажите автономный инсталляционный пакет Агента администрирования.

   - Если по какой-либо причине вам необходимо снова запустить мастер переноса данных, установите флажок **Загрузить автономный инсталляционный пакет** и нажмите на кнопку **Выберите автономный инсталляционный пакет**. В открывшемся окне браузера укажите автономный инсталляционный пакет Агента администрирования. После этого мастер переноса данных снова отображает иерархию групп администрирования этого Сервера администрирования. Выберите ту же группу, для которой вы создали файл экспорта, и нажмите на кнопку **Далее**.

     Мастер переноса данных снова проверяет общее количество управляемых устройств, включенных в выбранную группу администрирования. Если это количество превышает 10 000, появится сообщение об ошибке. Кнопка **Далее** остается неактивной до тех пор, пока количество управляемых устройств в выбранной группе администрирования будет меньше максимально допустимого значения.

2. Дождитесь загрузки автономного инсталляционного пакета и нажмите на кнопку **Далее**. Мастер переноса данных создает пользовательский инсталляционный пакет и задачу удаленной установки для него. Область действия задачи будет включать группу администрирования, которую вы выбрали на странице **Управляемые устройства для экспорта**; по умолчанию для времени запуска задачи установлено значение запуска **Вручную**. Мастер переноса данных отображает процесс создания пакета. Дождитесь пока значки (↻) будут заменены зелеными флажками (✓) и нажмите на кнопку **Далее**.

3. При необходимости установите флажок **Запустить только что созданную задачу удаленной установки** (по умолчанию флажок снят) для устройств в выбранной группе администрирования Сервера администрирования, работающего локально, и всех его подгрупп. В этом случае устройства будут переключаться под управление Kaspersky Security Center Cloud Console, но только после завершения установки Агента администрирования. Полный путь будет отображен для группы администрирования, в которой будет выполняться задача.

   Задачу нужно запускать только после завершения импорта в Kaspersky Security Center Cloud Console. Иначе устройства могут дублироваться.

4. Нажмите на кнопку **Готово**, чтобы закрыть мастер переноса данных и запустить задачу удаленной установки для следующих целей:

   - Обновление экземпляров Агента администрирования.
   - Переключение экземпляров Агента администрирования под управление Kaspersky Security Center Cloud Console.

   Если вы оставили снятым флажок **Запустить только что созданную задачу удаленной установки**, вы можете запустить задачу позже, если это необходимо.

Вы можете проверить, что теперь вы можете управлять перенесенными экземплярами Агента администрирования с помощью Kaspersky Security Center Cloud Console. Для этого перейдите в раздел **Управление активами** → **Активы (Устройства)**. Убедитесь, что на перенесенных управляемых устройствах есть значок подтверждения (⊙) в полях **Видимо в сети**, **Агент администрирования установлен** и столбцы **Агент администрирования запущен**. Также убедитесь, что на этих устройствах нет статуса с описанием *Давно не подключался*.

Перенос данных с иерархией Серверов администрирования

В этом разделе описывается перенос данных управляемых устройств и связанных с ними объектов из приложения Kaspersky Security Center Web Console, работающего локально, в Kaspersky Security Center Cloud Console. Процесс включает в себя иерархию: приложение Kaspersky Security Center Web Console, работающее локально, выполняет роль подчиненного Сервера администрирования, а Kaspersky Security Center Cloud Console выполняет роль главного Сервера администрирования.

Каждая группа администрирования, которую вы переносите в Kaspersky Security Center Cloud Console, должна содержать управляемые устройства одной операционной системы. Если ваша сеть включает устройства разных операционных систем, распределите их по разным группам администрирования, а затем перенесите каждую группу отдельно.

После завершения переноса данных все Агенты администрирования в группе, которая входит в область переноса данных, обновляются и переходят под управление Kaspersky Security Center Cloud Console.

Прежде чем начать, сделайте следующее:

- Обновите Сервер администрирования, работающий локально, до версии 14.2 или выше.
- Установите приложение Kaspersky Security Center Web Console версии 12.1 или выше.
- Обновите Агент администрирования на управляемых устройствах до версии 12 или выше.
- На устройствах с операционной системой Windows используйте Агент администрирования без пароля для деинсталляции.

  Если пароль уже задан, выполните одно из следующих действий в Kaspersky Security Center Web Console:

  - Выключите параметр **Использовать пароль деинсталляции** в свойствах политики Агента администрирования.
  - Удалите Агент администрирования удаленно с помощью задачи *Удаленная деинсталляция приложения*. В поле задачи **Приложение для деинсталляции** выберите значение **Агент администрирования Kaspersky Security Center**. Введите пароль для деинсталляции.
- Обновите управляемые приложения до версий, поддерживаемых Kaspersky Security Center Cloud Console.
- Убедитесь, что у вас есть политики для последних версий управляемых приложений. Если вы используете устаревшие политики, создайте политики для версий приложений, поддерживаемых Kaspersky Security Center Cloud Console.
- Чтобы использовать действующие политики, обновите веб-плагины для приложений, которыми вы планируете управлять с помощью Kaspersky Security Center Cloud Console.
- Удалите приложения "Лаборатории Касперского" с управляемых устройств, если эти приложения не поддерживаются Kaspersky Security Center Cloud Console.
- Расшифруйте все данные (на уровне диска или на уровне файлов), зашифрованные Kaspersky Endpoint Security для Windows на управляемых устройствах под управлением операционной системы Windows, и выключите функцию шифрования на управляемых устройствах с помощью политики приложения или локально. Дополнительную информацию см. в справке Kaspersky Endpoint Security для Windows.

  Если на устройстве с операционной системой Windows все еще хранятся какие-либо файлы или папки, зашифрованные с помощью Kaspersky Endpoint Security для Windows, обновление Агента администрирования будет отменено во время процесса переноса данных. Уведомление предложит вам расшифровать все данные на устройстве и отключить функцию шифрования.

Максимальное количество управляемых устройств на один Сервер администрирования в Kaspersky Security Center Cloud Console равно 25 000.

Чтобы выполнить перенос данных в Kaspersky Security Center Cloud Console:

1. Оцените область переноса данных, то есть просмотрите группу администрирования для экспорта, и оцените количество управляемых устройств в ней. Убедитесь, что все действия, перечисленные в качестве предварительных требований переноса данных, были успешно выполнены.
2. В Kaspersky Security Center Cloud Console перейдите на подчиненный Сервер администрирования для управляемых устройств, которые вы хотите перенести.

3. В главном окне приложения перейдите в раздел **Операции** → **Перенос данных**.

   Откроется страница приветствия мастера переноса данных.

4. На странице приветствия нажмите на кнопку **Далее**.

   Откроется страница **Управляемые устройства для экспорта**, на которой отображается вся иерархия групп администрирования подчиненного Сервера администрирования.

5. На странице **Управляемые устройства для экспорта** нажмите на значок шеврона (›) рядом с группой **Управляемые устройства** и раскройте иерархию групп администрирования. Выберите группу администрирования, которую вы хотите экспортировать.

   Мастер переноса данных выполняет проверку общего количества управляемых устройств, включенных в выбранную группу администрирования. Если это количество превышает 10 000, появится сообщение об ошибке. Кнопка **Далее** остается неактивной до тех пор, пока количество управляемых устройств в выбранной группе администрирования будет меньше максимально допустимого значения.

6. Выберите управляемые приложения, политики и задачи, которые необходимо перенести в Kaspersky Security Center Cloud Console вместе с объектами группы администрирования. Чтобы выбрать управляемые приложения, чьи объекты необходимо экспортировать, установите флажки рядом с их именами в списке.

   Несмотря на то, что Сервер администрирования Kaspersky Security Center есть в списке, установка соответствующего флажка не приводит к экспорту политик Сервера администрирования.

   Чтобы убедиться, что управляемые приложения поддерживаются Kaspersky Security Center Cloud Console, перейдите по ссылке. Ссылка перенаправит вас в раздел справки, содержащий список приложений, управляемых Kaspersky Security Center Cloud Console.

   Если вы выберете приложения, которые не поддерживаются приложением Kaspersky Security Center Cloud Console, политики и задачи этих приложений будут перенесены, но вы не сможете управлять ими в Kaspersky Security Center Cloud Console из-за недоступности плагинов.

7. Просмотрите список экспортируемых групповых объектов по умолчанию. При необходимости вы также можете указать объекты, не относящиеся к группе, которые будут экспортироваться вместе с выбранной группой администрирования, такие как глобальные задачи, пользовательские выборки устройств, отчеты, пользовательские роли, внутренние пользователи и группы безопасности, а также пользовательские категории программ, пополняемых вручную. Эта страница содержит следующие разделы:

   - **Глобальные задачи**

     Список глобальных задач управляемых приложений, а также глобальных задач Агента администрирования.

     Если выбранная вами глобальная задача применяется к определенной выборке объектов, эта выборка также будет экспортирована.

     Несмотря на то, что глобальные задачи Сервера администрирования есть в списке, вы не можете их экспортировать; выбор этих задач не влияет на область экспорта. Задачи удаленной установки также не входят в область экспорта, так как соответствующие инсталляционные пакеты невозможно экспортировать.

- **Выборки устройств**

  Список пользовательских выборок устройств.

- **Reports**

  Редактируемый список отчетов для экспорта.

  > Если выбранный вами отчет применяется к определенной выборке объектов, эта выборка также будет экспортирована.

  > Kaspersky Security Center Cloud Console содержит такой же набор шаблонов отчетов, как и Kaspersky Security Center Web Console, поэтому вы можете выбрать для экспорта только те отчеты, которые вы создали вручную или перенастроили.

- **Групповые объекты**

  Список групповых объектов для экспорта по умолчанию. Следующие объекты, связанные с выбранной группой администрирования, будут экспортированы полностью по умолчанию:

  - Структура группы администрирования, то есть все вложенные группы выбранной группы администрирования.
  - Устройства, которые были включены в группы администрирования для экспорта.
  - Теги, назначенные экспортируемым устройствам.

    > Если тег был создан в Kaspersky Security Center Web Console, но никогда не был назначен никакому устройству, он не будет экспортирован. Также правила автоматического назначения тегов не будут экспортированы.

  - Групповые политики выбранных управляемых приложений.

    > Политики Сервера администрирования и политики Агента администрирования не экспортируются.

  - Групповые задачи выбранных управляемых приложений и групповые задачи Агента администрирования.

    > Задачи Сервера администрирования не экспортируются.

Вы также можете запретить экспорт определенных типов объектов, не относящихся к группе:

- Чтобы отменить экспорт пользовательских ролей (то есть созданных только пользователем), установите флажок **Исключить пользовательские роли из экспорта**.
- Чтобы отменить экспорт для внутренних пользователей и групп безопасности, установите флажок **Исключить пользовательские роли и внутренние группы безопасности из экспорта**.
- Чтобы отменить экспорт пользовательских категорий приложений, пополняемых вручную, установите флажок **Исключить пользовательские категории приложений из экспорта**.

Если вы переносите устройства с различными операционными системами в Kaspersky Security Center Cloud Console, объекты, не относящиеся к группе, необходимо перенести только один раз.

8. После того как вы определили область переноса данных, нажмите на кнопку **Далее**, чтобы начать процесс экспорта. Откроется страница **Создание экспортного файла**, на которой можно просмотреть выполнение экспорта для каждого типа объектов, включенных в область переноса данных. Дождитесь пока каждый значок обновления (🔄) рядом с каждым пунктом в списке объектов заменится на зеленый флажок (✓). Экспорт заканчивается, файл экспорта автоматически сохраняется во временную папку. Откроется следующая страница, на которой отображается вся иерархия групп администрирования в приложении Kaspersky Security Center Cloud Console, выполняющее роль главного Сервера администрирования.

9. Установите флажок рядом с группой администрирования, в которую должны быть импортированы объекты группы, и нажмите на кнопку **Далее**. Файл распакован, а объекты, не относящиеся к группе, и объекты группы восстанавливаются в целевой группе администрирования.

   Если имя восстанавливаемого объекта совпадает с именем существующего объекта, к восстановленному будет добавлен дополнительный суффикс.

   Когда импорт завершится, экспортированная структура групп администрирования, включая сведения об устройствах, появится в целевой группе администрирования, которую вы выбрали. Объекты, не относящиеся к группе, также импортируются.

   Свернуть мастер переноса данных и выполнять любые параллельные операции во время импорта невозможно. Дождитесь, пока каждый значок обновления (🔄) рядом с каждым пунктом в списке объектов заменится на зеленый флажок (✓) и импорт завершится. После этого устройства начинают переключаться на Kaspersky Security Center Cloud Console.

10. После завершения импорта мастер переноса данных отобразит список инсталляционных пакетов Агента администрирования, доступных в Kaspersky Security Center Cloud Console для соответствующей операционной системы. Выберите инсталляционный пакет, содержащий соответствующую версию и локализацию Агента администрирования.

    Выберите инсталляционный пакет Агента администрирования для Windows, только если вы предварительно завершили мастер первоначальной настройки в рабочей области Kaspersky Security Center Cloud Console и если вы выполнили перенос данных для устройств под управлением операционной системы Windows.

11. Нажмите на кнопку **Далее**.

    Мастер переноса данных создает автономный инсталляционный пакет (или использует существующий) и пользовательский инсталляционный пакет на его основе, а также соответствующую задачу удаленной установки. Область действия задачи включает группу администрирования, выбранную вами на странице **Управляемые устройства для экспорта**. По умолчанию для времени запуска задачи установлено значение **Вручную**. Мастер переноса данных отображает процесс создания пакета.

12. Дождитесь, пока каждый значок обновления (🔄) заменится на зеленый флажок (✓) и нажмите на кнопку **Далее**.

13. При необходимости установите флажок **Запустить только что созданную задачу удаленной установки** (по умолчанию флажок снят) для устройств в выбранной группе администрирования приложения Kaspersky Security Center Web Console, работающего локально, и всех ее подгруппах. После завершения установки Агента администрирования вы можете управлять выбранными устройствами через Kaspersky Security Center Cloud Console. Полный путь отображается для группы администрирования, в которой будет выполняться задача.

    Задачу удаленной установки нужно запускать только после завершения импорта в Kaspersky Security Center Cloud Console. Иначе имена устройств могут дублироваться.

14. Нажмите на кнопку **Готово**, чтобы закрыть мастер переноса данных и запустить задачу удаленной установки для следующих целей:

    - Обновление экземпляров Агента администрирования.
    - Управление экземплярами Агента администрирования с помощью Kaspersky Security Center Cloud Console.

    Если вы оставили снятым флажок **Запустить задачу удаленной установки приложения**, вы можете запустить задачу позже, если это необходимо.

Вы можете проверить, что теперь вы можете управлять перенесенными экземплярами Агента администрирования с помощью Kaspersky Security Center Cloud Console. Для этого перейдите в раздел **Управление активами → Активы (Устройства)**. Убедитесь, что на перенесенных управляемых устройствах есть значок подтверждения (⊙) в полях **Видимо в сети**, **Агент администрирования установлен** и столбцы **Агент администрирования запущен**. Также убедитесь, что на этих устройствах нет статуса с описанием *Давно не подключался*.

Сценарий: перенос данных устройств с операционными системами Linux или macOS

В этом разделе описан перенос данных управляемых устройств с операционными системами Linux или macOS из приложения Kaspersky Security Center Web Console, работающего локально, в Kaspersky Security Center Cloud Console. Основные сценарии переноса данных без иерархии Серверов администрирования и сценарий переноса данных с такой иерархией позволяют переносить все устройства и связанные с ними объекты в Kaspersky Security Center Cloud Console. Если в вашей сети есть устройства, работающие не только под операционной системой Windows, но и под Linux или macOS, вам необходимо переносить устройства каждого типа операционной системы отдельно. В результате вам придется выполнять перенос данных несколько раз.

Предварительные требования

Прежде чем начать, сделайте следующее:

- Обновите Сервер администрирования, работающий локально, до версии 12 патч A или выше.
- Установите приложение Kaspersky Security Center Web Console версии 12.1 или выше.
- Обновите Агент администрирования на управляемых устройствах до версии 12 или выше.
- Обновите управляемые приложения до версий, поддерживаемых Kaspersky Security Center Cloud Console.
- Убедитесь, что у вас есть политики для последних версий управляемых приложений. Если вы используете устаревшие политики, создайте политики для версий приложений, поддерживаемых Kaspersky Security Center Cloud Console.
- Чтобы использовать действующие политики, обновите веб-плагины для приложений, которыми вы планируете управлять с помощью Kaspersky Security Center Cloud Console.
- Удалите приложения "Лаборатории Касперского" с управляемых устройств, если эти приложения не поддерживаются Kaspersky Security Center Cloud Console, а затем замените удаленные приложения на поддерживаемые.

Максимальное количество управляемых устройств на один Сервер администрирования в Kaspersky Security Center Cloud Console равно 25 000.

Этапы переноса данных

Перенос данных в Kaspersky Security Center Cloud Console включает в себя следующие этапы:

1. **Группировка управляемых устройств по их операционным системам**

   Если в вашей сети есть устройства под управлением разных операционных систем (Windows, Linux и macOS), разместите устройства с каждой операционной системой в отдельной группе администрирования в Kaspersky Security Center Web Console. Также создайте группу администрирования для каждого дистрибутива Linux. Например, если у вас есть устройства Debian и Red Hat Linux, распределите их по разным группам администрирования. Это позволит вам успешно выполнить перенос данных, так как для разных операционных систем требуются разные инсталлированные пакеты Агента администрирования.

2. **Выполнение переноса каждой группы администрирования и ее объектов**

   Управляемые устройства каждой операционной системы должны переноситься отдельно, чтобы включать их политики и задачи. Например, если у вас есть устройства с Windows, macOS, Ubuntu и CentOS, сначала перенесите устройства с операционной системой Windows в Kaspersky Security Center Cloud Console, затем macOS, Ubuntu и, наконец, в CentOS. Вы можете переносить управляемые устройства в любом порядке.

Для этого выполните перенос данных без иерархии Серверов администрирования или перенос данных с такой иерархией, в зависимости от того, есть ли в вашей сети подчиненные Серверы администрирования. При переносе данных используйте инсталляционный пакет Агента администрирования, соответствующий операционной системе переносимых устройств. Например, выберите Агент администрирования Kaspersky Security Center 13.2 для устройств Linux, чтобы перенос данных прошел успешно.

Обратите внимание, что негрупповые объекты, такие как глобальные задачи, пользовательские выборки устройств или отчеты, необходимо перенести только один раз.

Результаты

После завершения переноса данных вы можете убедиться, что перенос данных прошел успешно:

- Требуемая версия Агента администрирования переустанавливается на каждом управляемом устройстве под управлением операционной системы Linux или macOS.
- Все устройства с операционными системами Linux или macOS управляются через Kaspersky Security Center Cloud Console.
- Все параметры объектов, действовавшие до переноса данных, сохранились.

Сценарий: обратный перенос данных из Kaspersky Security Center Cloud Console в Kaspersky Security Center

Вам может потребоваться перенести данные управляемых устройств из Kaspersky Security Center Cloud Console на Сервер администрирования Kaspersky Security Center. Этот процесс можно использовать для отмены переноса данных в Kaspersky Security Center Cloud Console.

Предварительные требования

Убедитесь, что выполнены следующие предварительные требования:

- Приложение Kaspersky Security Center Cloud Console доступно и к нему подключены управляемые устройства.
- Сервер администрирования Kaspersky Security Center 14.2 (или выше) доступен и имеет инсталляционный пакет Агента администрирования версии 13 или выше.

Этапы обратного переноса данных

Обратный перенос данных включает в себя следующие этапы:

1. **Создание автономного инсталляционного пакета Агента администрирования на Сервере администрирования Kaspersky Security Center, работающего локально**

   На Сервере администрирования Kaspersky Security Center работающего локально, создайте автономный инсталляционный пакет Агента администрирования.

   В процессе создания вы можете выбрать параметр **Перемещать нераспределенные устройства в эту группу** и указать группу администрирования, в которую вы хотите переместить Агенты администрирования после установки. Если вы указали группу администрирования, будет создано правило автоматического перемещения устройств, которое переместит в целевую группу администрирования все Агенты администрирования с этим автономным инсталляционным пакетом.

   > Чтобы обеспечить обратный перенос данных без ошибок, убедитесь, что вы выбрали версию Агента администрирования не ниже, чем версия, используемая в Kaspersky Security Center Cloud Console.

2. **Создание пользовательского инсталляционного пакета в Kaspersky Security Center Cloud Console**

   В Kaspersky Security Center Cloud Console создайте пользовательский инсталляционный пакет на основе автономного инсталляционного пакета, который вы создали и сохранили на Сервере администрирования Kaspersky Security Center, запущенного локально.

   Чтобы включить установку пакета в тихом режиме, в поле **Параметры запуска исполняемого файла** укажите ключ `-s`.

3. **Создание задачи удаленной установки**

   В Kaspersky Security Center Cloud Console создайте задачу удаленной установки с помощью созданного вами пользовательского инсталляционного пакета.

4. **Запуск задачи удаленной установки приложения**

   Запустите задачу удаленной установки, которую вы создали. Задача инициирует переустановку всех Агентов администрирования в указанной группе администрирования; задача также переключает Агенты администрирования под управление Сервера администрирования Kaspersky Security Center, работающего локально, путем изменения адреса подключения и других параметров подключения.

   > Если вы не указали никакую целевую группу администрирования при создании автономного инсталляционного пакета, все устройства будут перемещены в группу **Нераспределенные устройства**.

Результаты

После завершения переноса данных вы можете убедиться, что перенос данных прошел успешно:

- Все устройства в области действия задачи удаленной установки, которые ранее управлялись через Kaspersky Security Center Cloud Console, теперь управляются Сервером администрирования Kaspersky Security Center, работающего локально.
- Устройства автоматически перемещаются в группу администрирования, указанную в параметрах инсталляционного пакета.

Задача удаленной установки в Kaspersky Security Center Cloud Console не может быть выполнена: нет целевых устройств, так как для всех устройств изменены параметры подключения. Вам нужно остановить задачу вручную после того, как убедитесь, что в столбце **Видимо в сети** списка управляемых устройств появился значок ошибки (!), для всех устройств из области переноса данных.

Перенос данных с виртуальными Серверами администрирования

Если у вас есть виртуальные Серверы администрирования в существующей инфраструктуре Kaspersky Security Center, вы не можете перенести данные из приложения Kaspersky Security Center, работающего локально, в Kaspersky Security Center Cloud Console с помощью мастера переноса данных. Также вы сможете выполнить перенос данных только для устройств ваших клиентов. Вам придется создать политики, задачи и отчеты вручную.

Вы можете выполнить один из следующих сценариев переноса данных:

- Переместив клиентские устройства с виртуальных Серверов администрирования на главный Сервер администрирования.
- Выполнив вручную перенос данных с виртуальных Серверов администрирования.

Сценарий: перенос данных с виртуальными Серверами администрирования с помощью перемещения устройств

Чтобы выполнить перенос данных из приложения Kaspersky Security Center Web Console, работающего локально, в Kaspersky Security Center Cloud Console, вы можете переместить свои устройства с виртуальных Серверов администрирования на главный Сервер администрирования.

Предварительные требования

Перед выполнением переноса данных вам нужно выполнить ряд действий, включая обновление Сервера администрирования, работающего локально, до версии 12 и выше и обновление управляемых приложений до версий, поддерживаемых приложением Kaspersky Security Center Cloud Console.

Сценарий переноса данных

Сценарий состоит из следующих этапов:

1. **Создание группы администрирования для каждого виртуального Сервера администрирования**

   Вы создаете группу в приложении Kaspersky Security Center, работающее локально.

2. **Переместите ваши клиентские устройства**

   Перемещение устройств клиентов с каждого виртуального Сервера администрирования в созданную на предыдущем этапе соответствующую группу администрирования, в приложении Kaspersky Security Center, работающем локально.

3. **Перенос данных**

   Выполните перенос данных, как описано для сети без иерархии виртуальных Серверов администрирования.

4. **Перемещение устройств под управление виртуальных Серверов администрирования (необязательный шаг)**

   Если вы хотите управлять своими клиентами с помощью виртуальных Серверов администрирования, переместите устройства из групп администрирования под управление виртуальных Серверов администрирования.

5. **Создание политик, задач и отчетов**

   Создайте требуемые политики, задачи и отчеты.

Результаты

После завершения переноса данных вы можете убедиться, что перенос данных прошел успешно:

- Агент администрирования перестановлен на всех управляемых устройствах.
- Все устройства управляются через Kaspersky Security Center Cloud Console.
- Все параметры объектов, действовавшие до переноса данных, сохранились.

Сценарий: перенос данных с виртуальными Серверами администрирования вручную

Вы можете выполнить перенос данных из приложения Kaspersky Security Center Web Console, работающего локально, в Kaspersky Security Center Cloud Console вручную.

Предварительные требования

Перед выполнением переноса данных вам нужно выполнить ряд действий, включая обновление Сервера администрирования, работающего локально, до версии 12 и выше и обновление управляемых приложений до версий, поддерживаемых приложением Kaspersky Security Center Cloud Console.

Сценарий переноса данных

Сценарий состоит из следующих этапов:

1. **Создание группы администрирования для каждого виртуального Сервера администрирования**

   Создайте группы администрирования, соответствующей каждому виртуальному Серверу администрирования, в Kaspersky Security Center Cloud Console.

2. **Создание автономного инсталляционного пакета Агента администрирования**

   Создайте автономный инсталляционный пакет Агента администрирования. Во время создания пакета укажите группу администрирования, созданную на предыдущем этапе. Вам нужно создать отдельный автономный инсталляционный пакет для каждой группы администрирования.

   Этот этап происходит в Kaspersky Security Center Cloud Console.

3. **Загрузка автономных инсталляционных пакетов**

   Загрузите автономные инсталляционные пакеты, которые вы создали на предыдущем этапе. Этот этап происходит в Kaspersky Security Center Cloud Console.

4. **Создание архива с каждым автономным инсталляционным пакетом**

   Доступные типы архивов: ZIP, CAB, TAR или TAR.GZ.

5. **Создание пользовательских инсталляционных пакетов Агента администрирования**

   Создайте пользовательские инсталляционные пакеты Агента администрирования. При создании используйте архивы, которые вы создали на предыдущем этапе.

   Этот этап выполняется в приложении Kaspersky Security Center, работающем локально.

6. **Создание задач удаленной установки**

   Создайте задачи удаленной установки приложений для установки Агента администрирования из созданных пользовательских инсталляционных пакетов.

   При создании задачи укажите соответствующую группу администрирования.

Этот этап выполняется в приложении Kaspersky Security Center, работающем локально.

7. **Запуск созданных задач удаленной установки приложений**

   Агенты администрирования обновлены. Агенты администрирования переключаются под управление Сервера администрирования Kaspersky Security Center Cloud Console.

   Выполнен перенос данных в Kaspersky Security Center Cloud Console и все устройства помещаются в группы администрирования, которые были указаны при создании автономных инсталляционных пакетов Агента администрирования.

8. **Перемещение устройств под управление виртуальных Серверов администрирования (необязательный шаг)**

   Если вы хотите управлять своими клиентами с помощью виртуальных Серверов администрирования, переместите устройства из групп администрирования под управление виртуальных Серверов администрирования.

9. **Создание политик, задач и отчетов**

   Создайте требуемые политики, задачи и отчеты.

Результаты

После завершения переноса данных вы можете убедиться, что перенос данных прошел успешно:

- Агент администрирования перестановлен на всех управляемых устройствах.
- Все устройства управляются через Kaspersky Security Center Cloud Console.

  Все параметры объектов, действовавшие до переноса данных, сохранились.

Сценарий: перемещение устройств из групп администрирования под управление виртуальных Серверов

Вы можете управлять своими клиентами с помощью виртуальных Серверов администрирования. Если вы перенесли устройства и другие объекты из приложения Kaspersky Security Center, работающего локально, в Kaspersky Security Center Cloud Console, устройства будут размещены в группах администрирования. Для управления устройствами клиентов с помощью виртуальных Серверов администрирования необходимо переместить устройства из групп администрирования под управление виртуальных Серверов администрирования.

Предварительные требования

У вас есть созданный виртуальный Сервер администрирования для каждого из ваших клиентов.

Все устройства каждого клиента находятся в отдельной группе администрирования.

Этапы

Сценарий состоит из следующих этапов:

1. **Создание автономного инсталляционного пакета Агента администрирования**

   Переключитесь на каждый из созданных виртуальных Серверов администрирования, затем создайте автономный инсталляционный пакет для Агента администрирования. Вы можете переключать Серверы администрирования в главном меню, нажав на значок шеврона (›) справа от имени текущего Сервера администрирования и выбрав требуемый Сервер администрирования.

2. **Загрузка автономных инсталляционных пакетов**

   Загрузите автономные инсталляционные пакеты, которые вы создали на предыдущем этапе.

3. **Создание архива с каждым автономным инсталляционным пакетом**

   Доступные типы архивов: ZIP, CAB, TAR или TAR.GZ.

4. **Создание пользовательских инсталляционных пакетов Агента администрирования**

   Создайте пользовательские инсталляционные пакеты Агента администрирования. При создании используйте архивы, которые вы создали на предыдущем этапе.

   Этот этап происходит на главном Сервере администрирования.

5. **Создание задач удаленной установки**

   Создайте задачи удаленной установки приложений для установки Агента администрирования из созданных пользовательских инсталляционных пакетов.

   При создании задачи укажите соответствующую группу администрирования.

   Этот этап происходит на главном Сервере администрирования.

6. **Запуск созданных задач удаленной установки приложений**

   Агенты администрирования обновлены. Устройства переданы под управление виртуальных Серверов администрирования.

7. **Создание политик, задач и отчетов**

   Создайте требуемые политики, задачи и отчеты.

Результаты

Теперь вы можете управлять перенесенными устройствами клиентов с помощью виртуальных Серверов администрирования.

Мастер первоначальной настройки

В этом разделе представлена информация о работе мастера первоначальной настройки Kaspersky Security Center Cloud Console.

О мастере первоначальной настройки

Мастер первоначальной настройки в Kaspersky Security Center Cloud Console позволяет создать минимальный набор необходимых задач и политик, настроить минимальный набор параметров и приступить к созданию инсталляционных пакетов приложений "Лаборатории Касперского". Используя мастер, вы можете внести в Kaspersky Security Center Cloud Console следующие изменения:

- Инициировать загрузку инсталляционных пакетов для управляемых приложений "Лаборатории Касперского".
- Создать автономный инсталляционный пакет Агента администрирования для устройств под управлением Windows, Linux или macOS.
- Создать политику Агента администрирования Kaspersky Security Center.
- Создать задачу *Загрузка обновлений в хранилища точек распространения*.
- Создать политики и задачи для управляемых приложений "Лаборатории Касперского".
- Настроить взаимодействие с Kaspersky Security Network (KSN).

После завершения работы мастера первоначальной настройки инсталляционные пакеты Агента администрирования и управляемых приложений "Лаборатории Касперского" появляются в списке **Обнаружение устройств и развертывание → Развертывание и назначение → Инсталляционные пакеты**.

Мастер первоначальной настройки создает политики для управляемых приложений, таких как Kaspersky Endpoint Security для Windows, если такие политики не были созданы в группе Управляемые устройства. Мастер первоначальной настройки создает задачи, если задачи с такими же именами не были созданы в группе Управляемые устройства.

Kaspersky Security Center Cloud Console автоматически предлагает запустить мастер первоначальной настройки после создания рабочей области организации и первого запуска Kaspersky Security Center Cloud Console. Вы также можете запустить мастер первоначальной настройки вручную в любое время.

Запуск мастера первоначальной настройки

Kaspersky Security Center Cloud Console автоматически предлагает запустить мастер первоначальной настройки после создания рабочей области организации и первого запуска Kaspersky Security Center Cloud Console. Вы также можете запустить мастер первоначальной настройки вручную в любое время.

При повторном запуске мастера первоначальной настройки задачи и политики, созданные при предыдущем запуске мастера, не создаются повторно.

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**.

3. Перейдите по ссылке **Запустить мастер первоначальной настройки**.

   Также можно запустить мастер первоначальной настройки, выбрав **Обнаружение устройств и развертывание → Развертывание и назначение → Мастер первоначальной настройки**.

Мастер предложит выполнить первоначальную настройку Kaspersky Security Center Cloud Console. Следуйте далее указаниям мастера. Для продолжения работы мастера нажмите на кнопку **Далее**. Используйте кнопку **Назад**, чтобы вернуться на предыдущий шаг мастера.

Шаг 1. Выбор инсталляционных пакетов для загрузки

В списке выберите приложения "Лаборатории Касперского" Kaspersky для установки на клиентские устройства. Kaspersky Security Center Cloud Console создаст инсталляционные пакеты для выбранных приложений. После этого вы будете использовать созданные инсталляционные пакеты для установки приложений.

При выборе инсталляционного пакета для загрузки обратите внимание на язык пакета: инсталляционные пакеты доступны на разных языках.

Выберите следующие приложения:

- Агент администрирования Kaspersky Security Center.

  При выборе инсталляционных пакетов Агента администрирования учитывайте следующее:

  - На каждом клиентском устройстве должен быть установлен Агент администрирования. Поэтому выберите Агент администрирования, подходящий для каждой операционной системы, установленной на клиентских устройствах.

  - Агент администрирования должен быть установлен вручную с помощью автономного инсталляционного пакета на устройстве, которое вы выбрали в качестве точки распространения. Точки распространения необходимы для опроса по сети и удаленной установки приложений безопасности "Лаборатории Касперского" на клиентские устройства. Поэтому необходимо выбрать хотя бы один инсталляционный пакет Агента администрирования. При переходе к следующим шагам мастера приложение Kaspersky Security Center Cloud Console создает автономный инсталляционный пакет Агента администрирования.

    По сравнению с точками распространения с операционной системой Windows, точки распространения с операционными системами Linux и macOS, имеют ограниченную функциональность. Рекомендуется выбирать компьютеры с операционной системой Windows в качестве точек распространения.

Вы можете выбрать Агенты администрирования для Windows, Linux и macOS. Если вы выберете Агент администрирования только для одной операционной системы, например, macOS, то для выбранной операционной системы будет создан автономный инсталляционный пакет. Если вы выберете Агент администрирования для нескольких операционных систем, Kaspersky Security Center Cloud Console создаст только один автономный инсталляционный пакет в соответствии со следующими приоритетами: Windows имеет самый высокий приоритет, далее Linux, а затем macOS. Например, если вы выберете Агенты администрирования для Linux и macOS, Kaspersky Security Center Cloud Console создаст автономный инсталляционный пакет Агента администрирования для Linux. Вы можете в любое время создать автономный инсталляционный пакет Агента администрирования для любой из этих операционных систем вручную.

- Приложения безопасности "Лаборатории Касперского".

  Выберите инсталляционные пакеты, соответствующие операционной системе, установленной на клиентских устройствах в вашей организации.

Шаг 2. Настройка параметров прокси-сервера

Если ваша организация использует прокси-сервер для подключения к интернету, укажите параметры прокси-сервера на этом шаге мастера. Эти параметры добавляются в инсталляционный пакет Агента администрирования. После установки Агент администрирования автоматически использует эти параметры на каждом клиентском устройстве.

Настройте следующие параметры подключения к прокси-серверу:

- **Использовать прокси-сервер**
- **Адрес**
- **Номер порта**
- **Аутентификация на прокси-сервере**

  Если этот параметр включен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  Рекомендуется указывать данные учетной записи с минимальными правами, необходимыми только для аутентификации на прокси-сервере.

  По умолчанию параметр выключен.

- **Имя пользователя**

  Имя пользователя учетной записи, от имени которой будет выполняться подключение к прокси-серверу.

  Рекомендуется указывать данные учетной записи с минимальными правами, необходимыми только для аутентификации на прокси-сервере.

- **Пароль**

  Пароль учетной записи, от имени которой будет выполняться подключение к прокси-серверу.

  Рекомендуется указывать данные учетной записи с минимальными правами, необходимыми только для аутентификации на прокси-сервере.

Шаг 3. Настройка Kaspersky Security Network

Если на первом шаге мастера вы загрузили инсталляционный пакет Kaspersky Endpoint Security для Windows, отображается текст Положения о KSN для следующих приложений:

- Kaspersky Endpoint Security для Windows;
- приложение Kaspersky Security Center, установленное на локальных устройствах;
- приложение Kaspersky Security Center Cloud Console, установленное в облачном окружении.

Если вы не загрузили инсталляционный пакет Kaspersky Endpoint Security для Windows, Положение о KSN для этого приложения не отображается.

В пробной версии отображается только Положение о KSN для Kaspersky Endpoint Security для Windows.

Внимательно прочитайте условия Положения о Kaspersky Security Network. Выберите один из следующих вариантов:

- **Я принимаю условия использования Kaspersky Security Network**

  Kaspersky Security Center Cloud Console 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 Cloud Console и управляемые приложения не будут предоставлять информацию о своей работе Kaspersky Security Network.

  Если вы выбрали этот параметр, использование Kaspersky Security Network будет выключено.

По умолчанию использование KSN выключено. Если в дальнейшем вы измените мнение по поводу использования KSN, можете включить (или выключить) соответствующий параметр в окне свойств Сервера администрирования в разделе **Прокси-сервер KSN**.

Шаг 4. Настройка управления обновлениями приложений сторонних производителей

Этот шаг не отображается, если задача *Поиск уязвимостей и требуемых обновлений*.

Если вы хотите получать список обновлений для приложений, установленных на управляемых устройствах, а также список обнаруженных уязвимостей и рекомендуемых исправлений для них, то включите параметр **Поиск обновлений приложений сторонних производителей и исправлений для уязвимостей**. Если параметр включен, Kaspersky Security Center Cloud Console создает задачу *Поиск уязвимостей и требуемых обновлений*.

Шаг 5. Создание базовой конфигурации защиты сети

На этом шаге мастера нажмите на кнопку **Создать**, чтобы создать объекты, необходимые для начальной защиты ваших клиентских устройств.

Kaspersky Security Center Cloud Console выполняет две операции:

- Создание основных политик и задач с параметрами по умолчанию.

  Созданы следующие политики:

  - политика Агента администрирования Kaspersky Security Center;
  - политики управляемых приложений "Лаборатории Касперского".

  Созданы следующие задачи:

  - Задачи *Загрузка обновлений в хранилища точек распространения*.
  - задача *Поиск уязвимостей и требуемых обновлений*.

    Эта задача создается, только если вы включили параметр **Поиск обновлений приложений сторонних производителей и исправлений для уязвимостей** на предыдущем шаге мастера.
  - Задачи для управляемых приложений "Лаборатории Касперского".

- Создание автономного инсталляционного пакета Агента администрирования

  Вы будете использовать этот пакет для установки Агента администрирования на точках распространения. Kaspersky Security Center Cloud Console создает автономный инсталляционный пакет на основе инсталляционного пакета Агента администрирования, выбранного вами на предыдущем шаге мастера. Во время создания пакета вам нужно прочитать и принять условия Лицензионного соглашения для Агента администрирования. Когда автономный инсталляционный пакет создан, отобразится предложение загрузить его на устройство, которое вы используете в данный момент.

  На создание автономного инсталляционного пакета Агента администрирования может потребоваться некоторое время. Перейдите к следующему шагу мастера. Процесс будет продолжен в фоновом режиме. Вы можете отслеживать статус загрузки инсталляционного пакета, а также фильтровать и сортировать статусы в столбце **Статус инсталляционного пакета** (**Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**).

Каждый автономный инсталляционный пакет подписывается с помощью сертификата для аутентификации. Сертификат перевыпускается каждые три месяца. После каждого переиздания сертификата Kaspersky Security Center Cloud Console автоматически обновляет подписи всех созданных автономных инсталляционных пакетов. Для загруженных автономных инсталляционных пакетов обновление подписи не может выполняться автоматически. Поэтому когда срок действия сертификата истекает, при установке приложения из автономного инсталляционного пакета, может возникнуть ошибка сертификата. В этом случае загрузите автономный инсталляционный пакет еще раз.

Также срок действия сертификата можно посмотреть в свойствах файла автономного инсталляционного пакета, загруженного на ваше устройство. Для этого нажмите правой кнопкой мыши на автономном инсталляционном пакете и перейдите к его сведениям. На вкладке **Цифровые подписи** в списке выберите нужный сертификат и нажмите на кнопку **Сведения**, далее в открывшемся окне нажмите на кнопку **Просмотр сертификата**.

Шаг 6. Завершение работы мастера первоначальной настройки

На странице завершения работы мастера первоначальной настройки ознакомьтесь с дополнительными операциями, которые необходимо выполнить для развертывания приложений безопасности "Лаборатории Касперского" на клиентских устройствах. Выполните этапы, предусмотренные в сценарии первоначального развертывания приложений "Лаборатории Касперского".

Первоначальное развертывание приложений "Лаборатории Касперского"

В этом разделе описано первоначальное развертывание приложений "Лаборатории Касперского" на клиентских устройствах в вашей организации.

Сценарий: первоначальное развертывание приложений "Лаборатории Касперского"

В этом сценарии описана установка приложений "Лаборатории Касперского" на клиентские устройства в Kaspersky Security Center Cloud Console. Сначала вам нужно развернуть точки распространения в своей сети. Затем с помощью точек распространения вам нужно выполнить опрос сети и обнаружить сетевые устройства в вашей сети. После этого вы можете развернуть приложения "Лаборатории Касперского" на сетевых устройствах.

После завершения сценария приложения "Лаборатории Касперского" будут развернуты на выбранных клиентских устройствах в сети организации. Вы можете управлять всеми устройствами с установленными приложениями "Лаборатории Касперского".

Предварительные требования

Убедитесь, что выполнены следующие предварительные требования:

- Мастер первоначальной настройки завершен.
- Агент администрирования и инсталляционные пакеты приложения безопасности созданы.
- У вас есть информация о параметрах подключения к интернету для клиентских устройств в вашей организации, информация о параметрах шлюза соединения и прокси-сервера.
- Клиентские устройства в вашей организации не зашифрованы.

Этапы

Первоначальное развертывание приложений "Лаборатории Касперского" состоит из следующих этапов:

1. **Выбор устройств, которые выполняют роль точек распространения**

В Kaspersky Security Center Cloud Console точка распространения предназначена для:

- опроса сети и обнаружения устройств;
- удаленной установки Агента администрирования на клиентские устройства;
- подключения клиентских устройств к Серверу администрирования (когда точка распространения выполняет роль шлюза соединения).

Выберите устройства в сети вашей организации, которые выполняют роль точек распространения для группы администрирования. Выбранные устройства должны отвечать требованиям для точек распространения. В зависимости от количества клиентских устройств в сети вашей организации выберите требуемое количество устройств на роль точек распространения.

2. **Создание автономного инсталляционного пакета Агента администрирования**

   Создайте автономный инсталляционный пакет Агента администрирования для установки на точку распределения.

   Если ваши клиентские устройства не имеют прямого доступа к Серверу администрирования через интернет, в параметрах инсталляционного пакета Агента администрирования настройте параметры шлюза соединения и прокси-сервера.

3. **Установка Агента администрирования на выбранное устройство, выполняющее роль точки распространения**

   Доставьте автономный инсталляционный пакет Агента администрирования на выбранное устройство любым способом. Например, вы можете скопировать автономный инсталляционный пакет на съемный диск (запоминающее устройство) или переместить его в папку общего доступа.

   В окне **Свойства** файла автономного инсталляционного пакета убедитесь, что автономный инсталляционный пакет для Агента администрирования подписан "Лабораторией Касперского".

   Запустите установку автономного инсталляционного пакета Агента администрирования на клиентском устройстве. Агент администрирования установлен с параметрами, указанными в инсталляционном пакете Агента администрирования, и подключен к Серверу администрирования. Устройство с Агентом администрирования перемещается в группу администрирования, которая была указана при создании автономного инсталляционного пакета для Агента администрирования.

   > Если вы устанавливаете Агент администрирования с помощью автономного инсталляционного пакета на устройство под управлением 32-разрядной версии Microsoft Windows XP Professional for Embedded Systems, установка завершится неудачно. Чтобы избежать этого, предварительно установите обновление KB2868626 для Windows XP, загрузив его с веб-сайта Microsoft: https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626.

4. **Назначение устройства с установленным Агентом администрирования точкой распространения**

   Назначьте устройства с установленным Агентом администрирования точкой распространения.

5. **Настройка и выполнение опроса сети точками распространения**

   Настройте опрос сети для точки распространения с установленным Агентом администрирования. Вы также можете настроить опрос сети в политике Агента администрирования.

   После завершения опроса сети по расписанию клиентские устройства, подключенные к вашей сети организации, обнаружены и помещены в группу **Нераспределенные устройства**.

6. **Создание инсталляционных пакетов для Агента администрирования и управляемых приложений "Лаборатории Касперского"**

   Если вы не запускали мастер первоначальной настройки или пропустили этап создания инсталляционных пакетов, создайте инсталляционные пакеты для приложений "Лаборатории Касперского". Вам нужно создать оба инсталляционных пакета, для Агента администрирования и для управляемых приложений "Лаборатории Касперского", соответствующие операционной системе, установленной на клиентских устройствах в вашей организации.

7. **Удаление приложений безопасности сторонних производителей**

   Если на клиентских устройствах в сети вашей организации установлены приложения безопасности сторонних производителей, удалите их перед установкой приложений "Лаборатории Касперского".

8. **Установка приложений "Лаборатории Касперского" на клиентские устройства**

   Создайте задачи для установки Агента администрирования и управляемых приложений "Лаборатории Касперского" на клиентские устройства в сети вашей организации. При создании задач используйте тип задачи **Удаленная установка приложения**. Для задачи установки Агента администрирования используйте параметр **Средствами операционной системы с помощью точек распространения**. Для задачи установки управляемых приложений "Лаборатории Касперского" используйте параметр **С помощью Агента администрирования**. После создания задач, вы можете настроить их параметры. Убедитесь, что расписание запуска каждой задачи соответствует вашим требованиям. Сначала должна быть запущена задача установки Агента администрирования. После установки Агента администрирования на клиентские устройства необходимо запустить задачу установки управляемых приложений "Лаборатории Касперского".

   Вы также можете создать одну задачу удаленной установки для установки Агента администрирования и управляемых приложений "Лаборатории Касперского" на клиентские устройства в сети вашей организации. В этом случае в блоке **Инсталляционные пакеты** используйте параметры **Выбор инсталляционного пакета** и **Выбор Агент администрирования**; в блоке **Принудительно скачать инсталляционный пакет** используйте параметр **Средствами операционной системы с помощью точек распространения**.

   Вы можете создать несколько задач удаленной установки чтобы установить управляемые приложения "Лаборатории Касперского" для различных групп администрирования или выборок устройств.

   Если у вас есть клиентские устройства, которые находятся вне сети с точкой распространения, например, ноутбуки автономных пользователей, вам нужно создать и доставить автономный инсталляционный пакет Агента администрирования на эти клиентские устройства любым способом. Установите автономный инсталляционный пакет Агента администрирования локально на эти клиентские устройства. Затем вы можете установить управляемые приложения "Лаборатории Касперского" на устройства этих автономных пользователей, следуя тем же инструкциям, что и для других устройств, обнаруженных точкой распространения.

   Запустите задачи удаленной установки приложений.

   Вы также можете запустить Мастер развертывания защиты, чтобы установить приложения "Лаборатории Касперского".

9. **Установка Kaspersky Security для мобильных устройств**

   Если вы планируете управлять корпоративными мобильными устройствами, см. справку Kaspersky Security для мобильных устройств информацию о развертывании Kaspersky Endpoint Security для Android.

10. **Проверка первоначального развертывания приложений "Лаборатории Касперского"**

    Сформируйте и просмотрите **Отчет о версиях приложений "Лаборатории Касперского"**. Убедитесь, что управляемые приложения "Лаборатории Касперского" установлены на всех клиентских устройствах в вашей организации.

Для полнодискового шифрования Kaspersky Security Center Cloud Console поддерживает только BitLocker.

Создание инсталляционных пакетов для приложений "Лаборатории Касперского"

Для развертывания приложений "Лаборатории Касперского" на сетевых устройствах вашей организации необходимо создать инсталляционные пакеты приложений "Лаборатории Касперского" в Kaspersky Security Center Cloud Console.

Чтобы создать инсталляционный пакет приложения "Лаборатории Касперского":

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
   - В главном окне приложения перейдите в раздел **Операции** → **Хранилища** → **Инсталляционные пакеты**.

   Вы также можете просматривать информацию о новых пакетах 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.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Выберите **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**.

   Отобразится список дистрибутивов доступных на веб-серверах "Лаборатории Касперского". 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.

4. Выберите требуемый дистрибутив, например, **Kaspersky Endpoint Security для Windows (<номер версии>)**.

   Откроется окно с информацией о дистрибутиве.

5. Ознакомьтесь с информацией и нажмите на кнопку **Скачать и создать инсталляционный пакет**.

   Если дистрибутив не может быть автоматически преобразован в инсталляционный пакет, вместо кнопки **Скачать и создать инсталляционный пакет** отображается кнопка **Скачать дистрибутив**. В этом случае загрузите дистрибутив, а затем используйте загруженный файл для создания пользовательского инсталляционного пакета.

Перед процессом загрузки или во время загрузки некоторых приложений "Лаборатории Касперского" отображается кнопка **Показать Лицензионное соглашение**. Если эта кнопка отображается:

a. Нажмите на кнопку **Показать Лицензионное соглашение**, чтобы прочитать Лицензионные соглашения.

b. В открывшейся панели прочтите Лицензионные соглашения, отображаемые на экране.

Чтобы просмотреть данные, обрабатываемые приложениями "Лаборатории Касперского", для которых вы хотите создать инсталляционный пакет, нажмите **Просмотреть список данных**.

c. Выберите Лицензионные соглашения и нажмите **Принять**.

Загрузка продолжится после принятия Лицензионных соглашений. Если вы нажмете на кнопку **Отклонить**, загрузка прекратится.

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.

По умолчанию инсталляционные пакеты со статусами **В процессе** и **Принять Лицензионное соглашение** располагаются в начале списка.

Если вы планируете выполнить перенос данных из Kaspersky Security Center Web Console в Kaspersky Security Center Cloud Console, использование прокси-сервера для доступа к корпоративной сети может повлиять на перенос данных. После того, как вы создадите инсталляционный пакет Агента администрирования, вам нужно указать параметры прокси-сервера, чтобы обеспечить соединение экземпляров Агента администрирования на управляемых устройствах с рабочей областью Kaspersky Security Center Cloud Console:

a. Нажмите на имя установочного пакета.

b. В открывшемся окне свойств инсталляционного пакета выберите вкладку **Параметры**.

c. Откройте раздел **Подключение**.

d. Выберите параметр **Использовать прокси-сервер** и заполните поля **Адрес прокси-сервера** и **Порт прокси-сервера**.

6. После завершения загрузки нажмите на кнопку **Закрыть** (), чтобы закрыть информационное окно дистрибутива.

Инсталляционный пакет создан. Инсталляционный пакет появится в списке инсталляционных пакетов.

Вы не можете добавить инсталляционный пакет с одним и тем же языком локализации несколько раз. Например, если вы уже добавили инсталляционный пакет Kaspersky Endpoint Security для Windows (английский), вы можете добавить инсталляционные пакеты Kaspersky Endpoint Security для Windows на других языках, кроме английского.

Распространение инсталляционных пакетов на подчиненные Серверы администрирования

Чтобы распространить инсталляционные пакеты на подчиненные Серверы администрирования:

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.

2. Запустите создание задачи распространения инсталляционного пакета на подчиненные Серверы администрирования одним из следующих способов:

   - Если вы хотите сформировать задачу для подчиненных Серверов выбранной группы администрирования, запустите создание групповой задачи для этой группы.

   - Если вы хотите сформировать задачу для набора подчиненных Серверов, запустите создание задачи для набора устройств.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

   В окне **Новая задача** мастера создания задачи, в поле **Тип задачи** выберите **Распространение инсталляционного пакета**. Вы также можете изменить имя задачи по умолчанию в поле **Название задачи**.

   На следующем шаге укажите подчиненные Серверы администрирования для области задачи и следуйте указаниям мастера создания задачи. В результате работы мастера создания задачи будет создана задача распространения выбранных инсталляционных пакетов на указанные подчиненные Серверы администрирования.

   > При создании задачи Распространение инсталляционного пакета для подчиненных Серверов администрирования, работающих локально, в область распространения, помимо пользовательских инсталляционных пакетов, будут включены только инсталляционные пакеты приложений "Лаборатории Касперского", которые поддерживаются приложением Kaspersky Security Center Web Console, работающим локально, – независимо от того, какой вариант распространения был выбран (**Все инсталляционные пакеты** или **Выбранные инсталляционные пакеты**).

3. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи выбранные инсталляционные пакеты будут скопированы на выбранные подчиненные Серверы администрирования.

Создание автономных инсталляционных пакетов Агента администрирования

Вы и пользователи устройств в вашей организации можете использовать автономные инсталляционные пакеты для локальной установки Агента администрирования на устройства. Автономный инсталляционный пакет может быть создан для устройств под управлением операционных систем Windows, Linux или macOS.

В Kaspersky Security Center Cloud Console вы можете создавать автономные инсталляционные пакеты только для Агента администрирования.

Автономный инсталляционный пакет представляет собой исполняемый файл, который можно отправить по почте или передать на клиентское устройство другим способом. Полученный файл можно запустить локально на клиентском устройстве, чтобы установить Агент администрирования без участия Kaspersky Security Center Cloud Console.

Для Агента администрирования для Linux и для Агента администрирования для macOS автономный инсталляционный пакет представляет собой файл сценария с расширением .sh. Когда вы запускаете этот файл сценария, выполняется распаковка вложенного архива, содержащего инсталляционный пакет и его параметры, а затем начинается установка.

Если Сервер администрирования имеет доступ в интернет, для загрузки зависимостей, необходимых для создания автономных инсталляционных пакетов Агента администрирования, используется задача **Загрузка обновлений в хранилище Сервера администрирования**. Если у Сервера администрирования нет доступа в интернет, выполните следующие действия:

1. Выполните следующую команду, чтобы создать флаг RIUtilsArchiveDirUsed:

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Выполните следующую команду, чтобы перезапустить службу Сервера администрирования:

   ```
   systemctl restart kladminserver_srv.service
   ```

Загрузите следующие архивы с сайта "Лаборатории Касперского" и поместите их в директорию /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives:

- ri_utils_win32.zip
- ri_utils_arm64.zip

Не переименовывайте архивы.

Теперь у Сервера администрирования есть нужные зависимости.

Если вы устанавливаете Агент администрирования с помощью автономного инсталляционного пакета на устройство под управлением 32-разрядной версии Microsoft Windows XP Professional for Embedded Systems, установка завершится неудачно. Чтобы избежать этого, предварительно установите обновление KB2868626 для Windows XP, загрузив его с веб-сайта Microsoft: https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626.

Каждый автономный инсталляционный пакет подписывается с помощью сертификата для аутентификации. Сертификат перевыпускается каждые три месяца. После каждого переиздания сертификата Kaspersky Security Center Cloud Console автоматически обновляет подписи всех созданных автономных инсталляционных пакетов. Для загруженных автономных инсталляционных пакетов обновление подписи не может выполняться автоматически. Поэтому когда срок действия сертификата истекает, при установке приложения из автономного инсталляционного пакета, может возникнуть ошибка сертификата. В этом случае загрузите автономный инсталляционный пакет еще раз.

Также срок действия сертификата можно посмотреть в свойствах файла автономного инсталляционного пакета, загруженного на ваше устройство. Для этого нажмите правой кнопкой мыши на автономном инсталляционном пакете и перейдите к его сведениям. На вкладке **Цифровые подписи** в списке выберите нужный сертификат и нажмите на кнопку **Сведения**, далее в открывшемся окне нажмите на кнопку **Просмотр сертификата**.

Чтобы создать автономный инсталляционный пакет:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
   - В главном окне приложения перейдите в раздел **Операции** → **Хранилища** → **Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов. Если инсталляционный пакет Агента администрирования отсутствует в списке, создайте этот инсталляционный пакет вручную.

2. В списке инсталляционных пакетов, нажмите на имя инсталляционного пакета Агента администрирования.

   Отобразится окно свойств инсталляционного пакета Агента администрирования.

3. При необходимости настройте параметры инсталляционного пакета Агента администрирования и закройте окно свойств инсталляционного пакета Агента администрирования.

4. В списке инсталляционных пакетов выберите пакет и над списком нажмите на кнопку **Развернуть**.

5. Выберите параметр **С использованием автономного инсталляционного пакета**.

   Запустится мастер создания автономного инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

6. 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.

7. На шаге **Перемещение в список управляемых устройств** параметр **Не перемещать устройства** выбран по умолчанию. Если вы не хотите перемещать клиентское устройство ни в какую группу администрирования после установки Агента администрирования, не изменяйте этот параметр.

   Если вы хотите переместить клиентское устройство после установки Агента администрирования, выберите параметр **Перемещать нераспределенные устройства в эту группу** и укажите группу администрирования, в которую вы хотите переместить клиентское устройство. По умолчанию устройства перемещаются в группу **Управляемые устройства**.

8. Выберите параметр **Открыть список автономных пакетов**, если вы хотите, чтобы список автономных инсталляционных пакетов отображался после завершения работы мастера.

9. Нажмите на кнопку **Готово**.

   Мастер создания автономного инсталляционного пакета закрывается.

Автономный инсталляционный пакет Агента администрирования создан. Созданный автономный инсталляционный пакет отображается в списке автономных инсталляционных пакетов, которые вы можете просмотреть.

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:

1. В главном окне приложения перейдите в раздел **Операции** → **Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов.

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

Отобразится список автономных инсталляционных пакетов.

Свойства автономных инсталляционных пакетов в списке отображаются следующим образом:

- **Имя пакета**. Имя автономного инсталляционного пакета, которое автоматически формируется из имени и версии приложения, включенной в пакет.
- **Имя инсталляционного пакета Агента администрирования**.
- **Версия Агента администрирования**.
- **Размер**. Размер файла в мегабайтах (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.
- **Хеш файла**. Это свойство используется для подтверждения того, что автономный инсталляционный пакет не был изменен сторонними лицами и у пользователя есть тот же файл, который вы создали и передали ему.

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:

- Удалить автономный инсталляционный пакет, нажав на кнопку **Удалить**.
- Загрузить автономный инсталляционный пакет на свое устройство, нажав на кнопку **Скачать**.

  Каждый автономный инсталляционный пакет подписывается с помощью сертификата для аутентификации. Сертификат перевыпускается каждые три месяца. После каждого переиздания сертификата Kaspersky Security Center Cloud Console автоматически обновляет подписи всех созданных автономных инсталляционных пакетов. Для загруженных автономных инсталляционных пакетов обновление подписи не может выполняться автоматически. Поэтому когда срок действия сертификата истекает, при установке приложения из автономного инсталляционного пакета, может возникнуть ошибка сертификата. В этом случае загрузите автономный инсталляционный пакет еще раз.

  Также срок действия сертификата можно посмотреть в свойствах загруженного автономного инсталляционного пакета. Для этого на вкладке **Цифровые подписи** в списке выберите нужный сертификат и нажмите на кнопку **Сведения**, далее в открывшемся окне нажмите на кнопку **Просмотр сертификата**.

Создание пользовательского инсталляционного пакета

Вы можете использовать пользовательские инсталляционные пакеты, чтобы:

- установить любое приложение (например, текстовый редактор) на клиентские устройства с использованием Kaspersky Security Center Cloud Console, например, с помощью задачи;
- создать автономный инсталляционный пакет.

Пользовательский инсталляционный пакет – это папка с набором файлов, включающая исполняемый файл. Источником для создания пользовательского инсталляционного пакета является архивный файл. Архивный файл содержит файл или файлы, которые должны быть включены в пользовательский инсталляционный пакет. Создавая пользовательский инсталляционный пакет, вы можете указать параметры командной строки, например для установки приложения в тихом режиме.

Вы не можете создать пользовательский инсталляционный пакет в пробном режиме Kaspersky Security Center Cloud Console.

Чтобы создать пользовательский инсталляционный пакет:

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
   - В главном окне приложения перейдите в раздел **Операции** → **Хранилища** → **Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Выберите **Создать инсталляционный пакет из файла**.
4. Укажите имя инсталляционного пакета и нажмите на кнопку **Обзор**.

   В стандартном окне **Открыть** можно выбрать архивный файл для создания инсталляционного пакета.
5. Выберите архивный файл, расположенный на доступных дисках.

   Вы можете загрузить архивный файл формата ZIP, CAB, TAR или TAR.GZ. Создать инсталляционный пакет из файла формата SFX (самораспаковывающийся архив) нельзя.

   Файлы загружены на Сервер администрирования Kaspersky Security Center Cloud Console.

   Если Сервер администрирования обнаружит, что в архив входит приложение "Лаборатории Касперского", отобразится сообщение об ошибке. Вы можете загрузить инсталляционные пакеты приложений "Лаборатории Касперского" с веб-серверов "Лаборатории Касперского". Эта операция доступна, если выбрать **Операции** → **Приложения "Лаборатории Касперского"** → **Текущие версии приложений**.

6. Если выбранный архивный файл включает в себя несколько исполняемых файлов, выберите один исполняемый файл, который необходимо запустить для установки приложения с использованием созданного инсталляционного пакета.

7. Если хотите, вы можете указать исполняемый файл в параметрах командной строки.

   Вы можете указать параметры командной строки для установки приложения из инсталляционного пакета в тихом режиме. Дополнительную информацию о параметрах командной строки см. в документации производителя.

   Начнется создание инсталляционного пакета.

   В окне мастера отобразится информация о завершении процесса.

   Если инсталляционный пакет не создан, отобразится сообщение об ошибке.

   В Kaspersky Security Center Cloud Console общий размер всех пользовательских инсталляционных пакетов на Сервере администрирования ограничен 500 МБ. Если этот предел превышен при создании нового пользовательского инсталляционного пакета, удалите более старые пользовательские инсталляционные пакеты, созданные ранее. Размер инсталляционного пакета отображается в его свойствах.

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

Созданный пользовательский инсталляционный пакет будет загружен на Сервер администрирования. После загрузки инсталляционный пакет появится в списке инсталляционных пакетов.

В списке инсталляционных пакетов вы можете просмотреть следующие свойства пользовательского инсталляционного пакета:

- **Имя**. Название инсталляционного пакета.
- **Статус инсталляционного пакета**. Статус скачивания инсталляционного пакета.
- **Источник**. Имя поставщика приложения.
- **Приложение**. Название приложения, упакованного в пользовательский инсталляционный пакет.
- **Версия**. Версия приложения.
- **Язык**. Язык приложения, упакованного в пользовательский инсталляционный пакет.
- **Размер (МБ)**. Размер пользовательского инсталляционного пакета.
- **ОС**. Операционная система, для которой создается пользовательский инсталляционный пакет.
- **Создано**. Дата создания инсталляционного пакета.
- **Изменено**. Дата изменения инсталляционного пакета.
- **Тип**. Приложение "Лаборатории Касперского" или приложение стороннего производителя.

Нажав на имя пользовательского инсталляционного пакета в списке инсталляционных пакетов, вы можете изменить параметры командной строки и имя пользовательского инсталляционного пакета.

Требования для точки распространения

Чтобы обрабатывать до 10 000 клиентских устройств, точка распространения должна отвечать следующим минимальным требованиям (предоставлена конфигурация тестового стенда):

- Процессор: Intel® Core™ i7-7700 CPU, 3,60 ГГц, 4 ядра.
- Оперативная память: 8 ГБ.
- Свободное место на диске: 120 ГБ.

Кроме того, точка распространения должна иметь доступ в интернет и должна быть всегда подключена.

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.

Параметры инсталляционного пакета Агента администрирования

Чтобы настроить параметры инсталляционного пакета Агента администрирования:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание → Развертывание и назначение → Инсталляционные пакеты**.
   - В главном окне приложения перейдите в раздел **Операции → Хранилища → Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. Перейдите по ссылке с названием инсталляционного пакета Агента администрирования.

   Отобразится окно свойств инсталляционного пакета Агента администрирования. Информация в окне сгруппирована по вкладкам и разделам.

Общие

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

- язык инсталляционного пакета;
- 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.

Параметры

В этом разделе можно настроить параметры, необходимые для обеспечения работоспособности Агента администрирования сразу после его установки. Параметры этого раздела доступны только для устройств под управлением Windows.

В блоке параметров **Папка назначения** можно выбрать папку на клиентском устройстве, в которую будет установлен Агент администрирования.

- **Устанавливать в папку по умолчанию**

  Если выбран этот вариант, Агент администрирования будет установлен в папку <Диск>:\Program Files\Kaspersky Lab\NetworkAgent. Если такой папки нет, она будет создана автоматически.

  По умолчанию выбран этот вариант.

- **Устанавливать в заданную папку**

  Если выбран этот вариант, Агент администрирования будет установлен в папку, указанную в поле ввода.

В блоке параметров ниже можно задать пароль для задачи удаленной деинсталляции Агента администрирования:

- **Использовать пароль деинсталляции**

  Если параметр включен, при нажатии на кнопку **Изменить** можно ввести пароль для удаления приложения (доступно только для Агента администрирования на устройствах под управлением операционных систем семейства Windows).

  По умолчанию параметр выключен.

- **Статус**

- **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 флажок установлен, все загруженные обновления и патчи для Агента администрирования будут устанавливаться автоматически.

  Если флажок снят, 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 флажок установлен.

Подключение

В этом разделе можно настроить параметры подключения Агента администрирования к Серверу администрирования:

- **Использовать UDP-порт**

  Номер UDP-порта

  В поле можно указать номер порта подключения Сервера администрирования к Агенту администрирования по протоколу UDP.

  По умолчанию номер UDP-порта – 15000.

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

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

  По умолчанию параметр включен.

- **Не использовать прокси-сервер**

- **Использовать прокси-сервер**

  Если этот параметр включен, для подключения Агента администрирования к Серверу администрирования и шлюзу соединений используется интернет-прокси-сервер.

  Адрес прокси-сервера

  Порт прокси-сервера

- **Аутентификация на прокси-сервере**

  Если этот параметр включен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

Рекомендуется указывать данные учетной записи с минимальными правами, необходимыми только для аутентификации на прокси-сервере.

По умолчанию параметр выключен.

Имя пользователя

Имя пользователя учетной записи, от имени которой будет выполняться подключение к прокси-серверу.

Рекомендуется указывать данные учетной записи с минимальными правами, необходимыми только для аутентификации на прокси-сервере.

Пароль

Пароль учетной записи, от имени которой будет выполняться подключение к прокси-серверу.

Рекомендуется указывать данные учетной записи с минимальными правами, необходимыми только для аутентификации на прокси-сервере.

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

Дополнительно

В этом разделе вы можете настроить способ использования шлюза соединения и виртуальной машины, а также указать регистрировать ли пользователя в качестве владельца устройства:

- **Подключаться к Серверу администрирования через шлюз соединения**

  Поддерживается только прямое подключение к шлюзу соединения. Параметр использования интернет-прокси-сервера, указанный в инсталляционном пакете, не применяется.

- **Адрес шлюза соединения**

- **Включить динамический режим для VDI**

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

  По умолчанию параметр выключен.

- **Оптимизировать параметры для VDI**

  Если параметр включен, в параметрах Агента администрирования выключены следующие функции:

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

  По умолчанию параметр выключен.

- **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.

Дополнительные компоненты

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

Теги

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

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

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

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

История ревизий

В этом разделе можно посмотреть историю ревизий инсталляционного пакета. Вы можете сравнивать ревизии, просматривать ревизии, сохранять ревизии в файл, добавлять и изменять описания ревизий.

Параметры инсталляционного пакета Агента администрирования доступны для конкретной операционной системы, которые приведены в таблице ниже.

Параметры инсталляционного пакета Агента администрирования

Раздел свойств	Windows	Mac	Linux
Общие	✓	✓	✓
Параметры	✓	—	—
Подключение	✓	✓ * кроме флажка **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**	✓ * кроме флажка **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**
Дополнительно	✓	✓	✓
Дополнительные компоненты	✓	✓	✓
Теги	✓	✓ * кроме правил автоматического назначения тегов	✓ * кроме правил автоматического назначения тегов
История ревизий	✓	✓	✓

Виртуальная инфраструктура

Kaspersky Security Center Cloud Console поддерживает работу с виртуальными машинами. Для защиты виртуальной инфраструктуры вам нужно установить Агент администрирования на каждую виртуальную машину.

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 Cloud Console, которая не очень полезна для виртуальных машин.

При установке Агента администрирования на виртуальную машину или на шаблон, из которого в дальнейшем будут получены виртуальные машины, рекомендуется выполнить следующие действия:

- если выполняется удаленная установка, в окне свойств инсталляционного пакета Агента администрирования (в разделе **Дополнительно**) выбрать параметр **Оптимизировать параметры для VDI**;
- если выполняется интерактивная установка с помощью мастера, в окне мастера выбрать параметр **Оптимизировать параметры Агента администрирования для виртуальной инфраструктуры**.

Выбор параметров изменит параметры Агента администрирования таким образом, чтобы по умолчанию (до применения политики) были выключены следующие функции:

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

Как правило, перечисленные функции не нужны на виртуальных машинах в силу того, что программное обеспечение и виртуальное аппаратное обеспечение на них единообразны.

Выключение функций обратимо. Если любая из выключенных функций все же нужна, ее можно включить при помощи политики Агента администрирования, или в локальных параметрах Агента администрирования. Локальные параметры Агента администрирования доступны из контекстного меню соответствующего устройства в Консоли администрирования.

Поддержка динамических виртуальных машин

Kaspersky Security Center Cloud Console 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. Динамическая виртуальная машина, с установленным Агентом администрирования, также добавляется в базу данных Сервера администрирования. После выключения этой 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

Kaspersky Security Center Cloud Console поддерживает копирование виртуальной машины с установленным Агентом администрирования или создание виртуальной машины из шаблона с установленным Агентом администрирования.

Агент администрирования может автоматически обнаруживать копирование виртуальных машин в следующих случаях:

- 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.

Использование Агента администрирования для Windows, Linux и macOS: сравнение

Агент администрирования для macOS и Linux имеет несколько функциональных ограничений по сравнению с Агентом администрирования для Windows. 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, macOS и Linux.

Сравнение функций Агента администрирования

Функция Агента администрирования	Windows	Linux	macOS
Установка			
Автоматическая установка обновлений и патчей для Агента администрирования	✓	✓	–
Автоматическое распространение ключа	✓	✓	✓
Установка вручную с помощью запуска инсталляторов приложений на устройствах	✓	✓	✓
Принудительная синхронизация	✓	✓	✓ За исключением push-сервера
Точка распространения			
Опрос сети	✓ • Опрос IP-диапазонов • Опрос сети Windows • Опрос контроллеров домена (Microsoft Active Directory)	✓ • Опрос IP-диапазонов • Опрос контроллеров домена (Microsoft Active Directory, Samba как Active Directory, FreeIPA, ALD Pro)	–
Запуск службы прокси-сервер KSN на стороне точки распространения	✓	✓	–

Функция Агента администрирования	Windows	Linux	macOS
Загрузка обновлений через серверы обновлений "Лаборатории Касперского" в хранилища точек распространения, которые распространяют обновления на управляемые устройства	✓	✓	— Точки распространения под управлением macOS не могут загружать обновления с серверов обновлений "Лаборатории Касперского". Если устройства с операционной системой macOS находятся в области действия задачи *Загрузка обновлений в хранилища точек распространения*, задача завершится со статусом *Сбой*, даже если она успешно завершилась на всех устройствах с операционной системой Windows.
Принудительная установка приложений	✓	С ограничением: невозможно выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой Linux.	С ограничением: невозможно выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой macOS.
Работа с приложениями сторонних производителей			
Удаленная установка приложений на устройства	✓	—	—
Обновления программного обеспечения	✓	—	—
Настройка обновлений операционной системы в политике Агента администрирования	✓	—	—
Просмотр информации об уязвимостях в приложениях	✓	—	—
Поиск уязвимостей в приложениях	✓	—	—
Инвентаризация программного обеспечения, установленного на устройствах	✓	✓	—
Виртуальные машины			
Установка Агента администрирования на виртуальные машины	✓	✓	✓
Оптимизация параметров для VDI	✓	✓	✓
Поддержка динамических виртуальных машин	✓	✓	✓
Другое			
Аудит действий на удаленном клиентском устройстве с помощью совместного доступа к рабочему столу Windows	✓	—	—
Управление перезагрузкой устройств	✓	—	—
Менеджер соединений	✓	✓	✓

Функция Агента администрирования	Windows	Linux	macOS
Профили соединения для автономных пользователей	✓	✓	✓
Удаленное подключение к рабочему столу клиентского устройства	✓	✓	✓

Следующие разделы отображаются в свойствах точки распространения, хотя соответствующие функции не поддерживаются Агентом администрирования для macOS:

- Источник обновлений
- Прокси-сервер KSN
- Windows-домены
- Active Directory
- IP-диапазоны
- Дополнительно
- Статистика

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 **Управление активами** → **Задачи**.
2. Нажмите на имя задачи удаленной установки, для которой вы хотите указать параметры, специфичные для Unix.

   Откроется окно свойств задачи.
3. Перейдите в раздел **Параметры 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 Cloud Console 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 Cloud Console 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 Cloud Console 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.

Замещение приложений безопасности сторонних производителей

Для установки приложений безопасности "Лаборатории Касперского" средствами Kaspersky Security Center Cloud Console может потребоваться удалить стороннее программное обеспечение, несовместимое с устанавливаемым приложением. Kaspersky Security Center Cloud Console 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. Вы можете найти этот параметр в мастере развертывания защиты. Если этот параметр включен, Kaspersky Security Center Cloud Console 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.

Возможности ручной установки приложений

Вы можете установить Агент администрирования на устройства локально, не используя Kaspersky Security Center Cloud Console. Для этого создайте автономный инсталляционный пакет для Агента администрирования, как описано в следующем разделе: Создание автономного инсталляционного пакета. Перенесите пакет на клиентское устройство и установите его. После завершения установки Агента администрирования вы можете использовать устройство в качестве точки распространения.

Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center Cloud Console

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 Cloud Console при условии, что на каждом устройстве есть учетные записи пользователей с правами локального администратора.

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 точек распространения.

Вам нужно указать учетную запись, имеющую доступ к административным ресурсам общего доступа admin$, в параметрах задачи удаленной установки.

Вы можете указать целевые устройства явно (списком), выбрав группу администрирования Kaspersky Security Center Cloud Console, которой они принадлежат, либо созданием выборки устройств по определенному условию. Время запуска установки определяется расписанием задачи. Если в свойствах задачи включен параметр **Запускать пропущенные задачи**, задача может запускаться сразу при включении устройств или при переносе их в целевую группу администрирования.

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 Cloud Console, отвечающей за сетевое взаимодействие. При этом должны выполняться следующие условия:

- Доступ к целевым устройствам осуществляется со стороны точки распределения.
- 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).

  Также TCP-порт 445 проверяется, чтобы определить тип операционной системы целевого устройства перед выполнением удаленной установки (если UDP-порт 137 недоступен).

  > 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 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 Cloud Console, 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.

Устройства выполняющие роль точек распространения должны соответствовать требованиям для точек распространения. Вам нужно убедиться, что точки распространения присутствуют в каждой из изолированных подсетей, на которых размещены целевые устройства.

Объем свободного места в разделе с папкой %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit должен многократно превосходить суммарный объем дистрибутивов устанавливаемых приложений.

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 расположен: **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**. Вы можете использовать этот инсталляционный пакет для установки приложения в дальнейшем.

- Создает и запускает задачу удаленной установки для набора устройств или для группы администрирования. Созданная задача удаленной установки хранится в разделе **Задачи**. Вы можете запустить эту задачу в дальнейшем вручную. Тип задачи – **Удаленная установка приложения**.

Шаг 1. Запуск мастера развертывания защиты

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 способ установки выбранного инсталляционного пакета:

- **Удаленная установка с помощью Kaspersky Security Center**

- **Удаленная установка с помощью Microsoft Azure API**

Далее 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.

Шаг 3. 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 Kaspersky Security Center.

Выберите последнюю версию Агента администрирования.

Шаг 4. Выбор устройств

Укажите список устройств, на которые требуется установить приложение:

- **Установить на управляемые устройства**

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

- **Выбор устройств для установки**

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

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

Шаг 5. Задание параметров задачи удаленной установки

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

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

- **С помощью Агента администрирования**

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

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

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

  По умолчанию параметр включен.

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

  Если 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.

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.

Пароль для удаления приложения "Лаборатории Касперского"

> Поле **Пароль для удаления приложения "Лаборатории Касперского"** доступно, только если вы выбрали параметр **С помощью Агента администрирования** в группе параметров **Принудительно скачать инсталляционный пакет**.

Введите пароль в поле **Пароль для удаления приложения "Лаборатории Касперского"**, если вы переносите данные из одного приложения "Лаборатории Касперского" в другое и ваше текущее приложение защищено паролем. Обратите внимание, что во время переноса данных ваше текущее приложение "Лаборатории Касперского" будет удалено.

Для успешного завершения сценария переноса данных убедитесь, что выполнены следующие предварительные условия:

- Вы используете Агент администрирования Kaspersky Security Center для Windows версии 14.2 или выше.
- Вы устанавливаете приложение на устройства под управлением Windows.

Шаг 6. Управление перезагрузкой

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

- **Не перезагружать устройство**

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **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.

Шаг 7. Удаление несовместимых приложений перед установкой

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

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

Отображается список несовместимых приложений.

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

Шаг 8. Перемещение устройств в папку Управляемые устройства

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

- **Не перемещать устройства**

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

- **Перемещать нераспределенные устройства в группу**

  Устройства перемещаются в выбранную вами группу администрирования.

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

Шаг 9. Выбор учетных записей для доступа к устройствам

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 Cloud Console поддерживает формат закрытых ключей PEM, а утилита ssh-keygen по умолчанию генерирует SSH-ключи в формате OPENSSH. Формат OPENSSH не поддерживается Kaspersky Security Center Cloud Console. Чтобы создать закрытый ключ в поддерживаемом формате PEM, добавьте параметр -m PEM в команду ssh-keygen. Например:

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

Шаг 10. Запуск установки

Это последний шаг мастера. На этом шаге **Задача удаленной установки 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 **ОК**, чтобы завершить последний шаг мастера развертывания защиты.

Сетевые параметры для взаимодействия с внешними сервисами

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

Сетевые параметры	Адрес	Описание
Порт: 443 Протокол: HTTPS	activation-v2.kaspersky.com	Активация приложения.
Порт: 443 Протокол: HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	Обновление баз, 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 Cloud Console 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	ds.kaspersky.com dc1.ksn.kaspersky-labs.com dc1-file.ksn.kaspersky-labs.com dc1-pp.ksn.kaspersky-labs.com dc1-st.ksn.kaspersky-labs.com	Использование Kaspersky Security Network.
Порт: 443, 1443 Протокол: HTTPS	ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	Использование Kaspersky Security Network.
Порт: 443 Протокол: HTTPS	click.kaspersky.com redirect.kaspersky.com	Переход по ссылкам из интерфейса.
Порт: 80 Протокол: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Инфраструктура открытых ключей (Public Key Infrastructure, PKI).
Порт: 443 Протокол: HTTPS	https://ipm-klca.kaspersky.com	Рекламные объявления.

Сетевые параметры	Адрес	Описание
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).

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 Cloud Console 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 устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux

Установка Агента администрирования состоит из двух шагов:

- Подготовка устройства с операционной системой Linux
- Удаленная установка Агента администрирования

Подготовка устройства с операционной системой Linux

Чтобы подготовить устройство с операционной системой Linux к удаленной установке Агента администрирования:

1. Убедитесь, что на устройстве, на которое вы хотите установить Агент администрирования Linux, работает один из поддерживаемых дистрибутивов Linux.
2. Загрузите инсталляционный пакет Агента администрирования с помощью интерфейса приложения или с веб-сайта "Лаборатории Касперского".

   Если требуется установить Kaspersky Industrial CyberSecurity for Linux Nodes на устройство под управлением операционной системы Linux с glibc 2.5, скачайте один из следующих инсталляционных пакетов с сайта "Лаборатории Касперского":

   - klnagent64_16.1.0-5840_amd64_glibc2.5.deb
   - klnagent64-16.1.0-5840.x86_64_glibc2.5.rpm
   - klnagent_16.1.0-5840_i386_glibc2.5.deb
   - klnagent-16.1.0-5840.i386_glibc2.5.rpm

   Эти инсталляционные пакеты доступны для следующих операционных систем с glibc 2.5:

   - CentOS 5.2 32-разрядная/64-разрядная.
   - CentOS 5.4 32-разрядная/64-разрядная.
   - CentOS 6.4 32-разрядная/64-разрядная.
   - CentOS 6.6 32-разрядная/64-разрядная.
   - Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.4) 64-разрядная.

Для получения инсталляционного пакета у вас должна быть лицензия Kaspersky Industrial CyberSecurity for Linux Nodes.

3. 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.

4. 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`.

      Убедитесь, что порт TCP 22 открыт и доступен на нераспределенном устройстве под управлением ОС Linux. Для успешной установки Агента администрирования для Linux должен быть доступен TCP-порт 22.

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

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

      В открывшемся файле добавьте следующую строку в конец файла: `<имя пользователя> ALL = (ALL) NOPASSWD: ALL`. В этом случае `<имя пользователя>` является учетной записью пользователя, которая будет использоваться для подключения к устройству по протоколу SSH. Если вы используете операционную систему Astra Linux, в файл /etc/sudoers добавьте последней строку со следующим текстом: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

   d. Сохраните и закройте файл sudoers.

   e. Повторно подключитесь к устройству через SSH и проверьте, что служба sudo не требует пароль, с помощью команды `sudo whoami`.

5. Откройте файл `/etc/systemd/logind.conf` и выполните одно из следующих действий:

   - Укажите значение 'no' для параметра KillUserProcesses: `KillUserProcesses=no`.
   - Для параметра KillExcludeUsers введите имя пользователя учетной записи, под которой будет выполняться удаленная установка, например, `KillExcludeUsers=root`.

Если целевое устройство работает под управлением Astra Linux, добавьте строку `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` в файл `/home/< имя пользователя >/.bashrc`, где `< имя пользователя >` – учетная запись пользователя, которая будет использоваться для подключения устройства с помощью SSH.

Чтобы применить измененный параметр, перезапустите устройство под управлением Linux или выполните команду:

```
sudo systemctl restart systemd-logind.service
```

6. 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.

7. 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.

8. 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.

Удаленная установка Агента администрирования

Чтобы установить Агент администрирования на устройство с операционной системой Linux:

1. Загрузите и создайте инсталляционный пакет:

   a. Перед установкой пакета на устройство убедитесь, что на нем установлены зависимости (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 приложений с помощью задачи удаленной установки

Kaspersky Security Center Cloud Console позволяет удаленно устанавливать приложения на устройства с помощью задач удаленной установки. Эти задачи создаются и назначаются устройствам с помощью специального мастера. Чтобы быстрее и проще назначить задачу устройствам (до 1000 устройств), вы можете указывать в окне мастера устройства удобным для вас способом:

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

Для 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 Cloud Console.

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 **Управление активами** → **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 NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

  Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить 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.

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:

   - Выберите, как вы хотите установить выбранное приложение:

     - **Удаленная установка с помощью Kaspersky Security Center**

     - **Удаленная установка с помощью Microsoft Azure API**

       Дополнительные сведения об установке приложений на виртуальные машины Microsoft Azure см. в разделе Удаленная установка приложений на виртуальные машины Azure.

   - 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.

- 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 Cloud Console больше не запускает приложение установки на устройстве. Чтобы перезапустить задачу *Удаленная установка приложения*, увеличьте значение параметра **Максимальное количество попыток установок** и перезапустите 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 приложений может привести к ошибкам 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 дополнительные параметры:
  - **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 Cloud Console проверяет, применимы ли параметры утилиты установки к операционной системе клиентского устройства. Если параметры не применимы, Kaspersky Security Center Cloud Console 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 точка распространения автоматически определяет тип операционной системы устройства независимо от параметра **Предварительно проверять тип операционной системы перед загрузкой**.

  - **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.

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

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.

- **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.

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 Cloud Console поддерживает формат закрытых ключей PEM, а утилита ssh-keygen по умолчанию генерирует SSH-ключи в формате OPENSSH. Формат OPENSSH не поддерживается Kaspersky Security Center Cloud Console. 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.

Установка приложений на подчиненные Серверы администрирования

Чтобы установить приложение на подчиненные Серверы администрирования:

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.

2. Убедитесь в том, что соответствующий устанавливаемому приложению инсталляционный пакет находится на каждом из выбранных подчиненных Серверов администрирования. Если вы не можете найти инсталляционный пакет ни на одном из подчиненных Серверов, распространите его. Для этого создайте задачу с типом задачи **Распространение инсталляционного пакета**.

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.

Запуск и остановка приложений "Лаборатории Касперского"

Вы можете использовать задачу *Запуск и остановка приложений* 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 **Управление активами** → **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.

4. В списке **Тип задачи** выберите задачу **Запуск и остановка 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.

Чтобы запустить задачу, выберите задачу в списке задач и нажмите на кнопку **Запустить**.

Управление мобильными устройствами

Управление защитой мобильных устройств через Kaspersky Security Center Cloud Console выполняется с помощью компонента Управление мобильными устройствами. Если вы планируете управлять мобильными устройствами, принадлежащими сотрудникам вашей организации, включите и настройте Управление мобильными устройствами.

Управление мобильными устройствами позволяет управлять Android-устройствами сотрудников. Защиту обеспечивает мобильное приложение Kaspersky Security для мобильных устройств, установленное на устройствах. Это мобильное приложение обеспечивает защиту мобильных устройств от веб-угроз, вирусов и других приложений, которые представляют собой угрозы.

iOS-устройства

Kaspersky Device Management для iOS обеспечивает защиту и контроль мобильных устройств, подключенных к Kaspersky Security Center Cloud Console.

Приложение Kaspersky Security for iOS предлагает следующие основные функции:

- **Веб-Защита**. Этот компонент блокирует вредоносные сайты, созданные для распространения вредоносного кода. Веб-Защита также блокирует поддельные (фишинговые) сайты, созданные для кражи конфиденциальных данных пользователя (например, паролей для онлайн-банкинга или систем электронных денег) и доступа к финансовой информации пользователя.

- **Обнаружение jailbreak**. Когда приложение Kaspersky Security for iOS обнаруживает jailbreak, оно отображает критическое сообщение и информирует вас о проблеме.

Информацию о развертывании защиты и управлении мобильными устройствами см. в справке Kaspersky Security для мобильных устройств (cloud).

Возможности обнаружения и реагирования

Kaspersky Security Center Cloud Console может интегрировать функции других решений "Лаборатории Касперского" в интерфейсе консоли. Например, вы можете добавить функции обнаружения и реагирования к функциональности Kaspersky Security Center Cloud Console.

Решение обнаружения и реагирования предназначено для защиты ИТ-инфраструктуры организации от сложных киберугроз. Функциональность решения сочетает в себе автоматическое обнаружение угроз с возможностью реагирования на эти угрозы для защиты от сложных атак, включая новые эксплойты, приложения-шантажисты, бесфайловые атаки и методы, использующие законные системные инструменты.

Решения, которые можно интегрировать

Kaspersky Endpoint Detection and Response Optimum

После того, как приложение Kaspersky Endpoint Protection Platform (также называемое EPP) обнаруживает угрозу, Kaspersky Security Center Cloud Console добавляет алерт в список алертов. Алерт содержит подробную информацию об обнаруженной угрозе и позволяет анализировать и исследовать ее. Также вы можете визуализировать угрозы, создав график цепочки развития угроз. График описывает этапы развертывания обнаруженной атаки во времени.

В качестве реагирования можно выбрать одно из предопределенных действий по реагированию, например, переместить файл на карантин, изолировать взломанное устройство от сети или создать правило предотвращения выполнения для ненадежного объекта.

Для получения информации об активации решения см. документацию Kaspersky Endpoint Detection and Response Optimum.

Kaspersky Managed Detection and Response

После того, как EPP-приложение "Лаборатории Касперского" обнаруживает угрозу, Kaspersky Security Center Cloud Console добавляет новый инцидент в список инцидентов. Инцидент содержит подробную информацию об обнаруженной угрозе. Аналитики MDR Security Operation Center (SOC) "Лаборатории Касперского" или сторонней компании исследуют инциденты и предлагают меры по их устранению. Вы можете принять или отклонить предложенные меры вручную или включить параметр автоматического принятия всех ответов.

Информация об активации решения приведена в документации Kaspersky Managed Detection and Response.

Kaspersky Endpoint Detection and Response Expert

Это решение для организаций, в которых есть команда аналитиков SOC. Обнаруженные угрозы регистрируются как алерты или инциденты, которые можно передать на исследование аналитикам SOC. Kaspersky Endpoint Detection and Response Expert предоставляет вам подробную информацию о каждом алерте или инциденте, а также инструменты для управления алертами и инцидентами, поиска угроз и разработки пользовательских правил. Аналитики SOC или специалисты по безопасности могут вручную выбрать ответные действия или принять заранее определенные автоматизированные меры реагирования.

Информацию об активации решения см. в документации Kaspersky Endpoint Detection and Response Expert.

Изменения интерфейса после интеграции функций обнаружения и реагирования

В таблице ниже перечислены изменения, которые решения вносят в интерфейс Kaspersky Security Center Cloud Console после интеграции.

Изменения в интерфейсе после интегрирования решений "Лаборатории Касперского"

Решение	Изменения Kaspersky Security Center Cloud Console
Kaspersky EDR Optimum	Добавляются следующие элементы: • Раздел **Алерты** (**Мониторинг → Алерты**). Алерты, которые были найдены с помощью этого решения, отображаются на вкладке **Optimum**. • Виджет на вкладке **Панель мониторинга** (**Мониторинг → Панель мониторинга**).
Kaspersky MDR	Добавляются следующие элементы: • Раздел **MDR** (**Мониторинг → MDR**). • Параметр **Показать функции MDR** (**Параметры → Параметры интерфейса → Показать функции MDR**). • Виджет на вкладке **Панель мониторинга** (**Мониторинг → Панель мониторинга**).
Kaspersky EDR Expert	Добавляются следующие элементы: • Раздел **Алерты** (**Мониторинг → Алерты**). Алерты, которые были найденные с помощью этого решения, отображаются на вкладке **Expert**. • Раздел **Инциденты** (**Мониторинг → Инциденты**). • Раздел **Поиск угроз** (**Мониторинг → Поиск угроз**). • Раздел **Пользовательские правила** (**Мониторинг → Пользовательские правила**). • Общие параметры Kaspersky EDR Expert (**Параметры → Интеграция → Kaspersky EDR Expert**). • Виджет в разделе **Панель мониторинга** (**Мониторинг → Панель мониторинга**).

Data Discovery

В этом разделе приведена информация о Data Discovery.

О Data Discovery

Kaspersky Security Center Cloud Console обнаруживает важную информацию в файлах, находящихся в облачных хранилищах Microsoft 365. Можно просмотреть информацию о каждом обнаруженном файле: имя, тип совместного использования (частный, внутри или за пределами компании) и кто вносил в файл последние изменения.

Эта функция доступна, только если вы активировали Kaspersky Security Center Cloud Console по лицензии Kaspersky Next EDR Optimum или XDR Expert.

Приступить к использованию функции Data Discovery можно при первом запуске Консоли управления Kaspersky Security Center Cloud Console или после обновления Kaspersky Security Center Cloud Console до новой версии. Если вы не включили использование Data Discovery во время первоначальной или дополнительной настройки Kaspersky Security Center Cloud Console, можно включить его позже. После того, как вы начнете использовать эту функцию, подключите вашу организацию Microsoft 365 к рабочей области.

Виджет и таблица Data Discovery показывают обнаружения важной информации в файлах. Виджет показывает до 5 обнаруженных файлов, а таблица – до 1000 обнаружений.

Из таблицы Data Discovery можно экспортировать информацию обо всех текущих обнаружениях в файл CSV.

Если вы хотите прекратить использование этой функции, вы можете выключить ее. В дальнейшем ее можно включить повторно.

Если после начала использования Data Discovery вы удалили рабочую область или выключили эту функцию и больше не хотите ее использовать, перейдите в Microsoft 365 и вручную отзовите разрешения, предоставленные приложению **Kaspersky Security Center Cloud Console – DLP scanner**.

Категории информации, обнаруживаемой Data Discovery

Kaspersky Security Center Cloud Console обнаруживает важную информацию следующих категорий:

- Номер кредитной/дебетовой карты
- Персональные данные (Аргентина):
  - Водительское удостоверение (Аргентина)
  - Удостоверение личности (Аргентина)

    - Паспорт (Аргентина)
    - Уникальный номер налогоплательщика (Аргентина)
- Персональные данные (Бразилия):
    - Водительское удостоверение (CNH) (Бразилия)
    - Удостоверение личности (RG) (Бразилия)
    - Индивидуальный номер в реестре налогоплательщиков (CPF) (Бразилия)
    - Паспорт (Бразилия)
- Персональные данные (Чили):
    - Водительское удостоверение (Чили)
    - Удостоверение личности (Чили)
    - Паспорт (Чили)
    - Уникальный номер налогоплательщика (Чили)
- Персональные данные (Колумбия):
    - Водительское удостоверение (Колумбия)
    - Удостоверение личности (Колумбия)
    - Паспорт (Колумбия)
    - Уникальный номер налогоплательщика (NIT) (Колумбия)
- Персональные данные (Египет):
    - Водительское удостоверение (Египет)
    - Национальное удостоверение личности (Египет)
    - Паспорт (Египет)
- Персональные данные (ОАЭ):
    - Удостоверение личности (ОАЭ)
    - Паспорт (ОАЭ)
    - Водительское удостоверение (ОАЭ)
    - Единый номер (ОАЭ)

- Персональные данные (Франция):
  - Водительское удостоверение (Франция)
  - Удостоверение личности (Франция)
  - Паспорт (Франция)
  - Номер социального страхования (Франция)
- Персональные данные (Германия):
  - Водительское удостоверение (Германия)
  - Удостоверение личности (Германия)
  - Паспорт (Германия)
  - Разрешение на пребывание (Германия)
  - Номер социального страхования (Германия)
  - Идентификационный номер налогоплательщика (Германия)
- Персональные данные (Индия):
  - Водительское удостоверение (Индия)
  - Идентификационный номер плательщика налога на товары и услуги (Индия)
  - Уникальный идентификационный номер (Aadhaar) (Индия)
  - Паспорт (Индия)
  - Идентификационный номер налогоплательщика (Индия)
  - Удостоверение личности избирателя (Индия)
- Персональные данные (Италия):
  - Водительское удостоверение (Италия)
  - Идентификационный номер налогоплательщика (Италия)
  - Удостоверение личности (Италия)
  - Паспорт (Италия)
- Персональные данные (Малайзия)
  - Удостоверение личности (Малайзия)
  - Идентификационный номер налогоплательщика (Малайзия)
  - Водительское удостоверение (Малайзия)

- Персональные данные (Мексика):
  - Удостоверение личности (CURP) (Мексика)
  - Индивидуальный номер в реестре налогоплательщиков (RFC) (Мексика)
  - Паспорт (Мексика)
  - Номер социального страхования (Мексика)
- Персональные данные (Перу)
  - Национальное удостоверение личности (DNI) (Перу)
  - Идентификационный номер налогоплательщика (RUC) (Перу)
  - Водительское удостоверение (Перу)
  - Вид на жительство (Перу)
- Персональные данные (Португалия):
  - Удостоверение личности (Португалия)
  - Водительское удостоверение (Португалия)
  - Паспорт (Португалия)
  - Номер социального страхования (NISS) (Португалия)
  - Идентификационный номер налогоплательщика (NIF) (Португалия)
- Персональные данные (Саудовская Аравия):
  - Водительское удостоверение (Саудовская Аравия)
  - Национальная ID-карта (Саудовская Аравия)
  - Вид на жительство (Саудовская Аравия)
  - Паспорт (Саудовская Аравия)
- Персональные данные (Южная Африка)
  - Паспорт (Южная Африка)
  - Удостоверение личности (Южная Африка)
  - Уникальный номер налогоплательщика (Южная Африка)
- Персональные данные (Испания):
  - Удостоверение личности (Испания)
  - Номер социального страхования (Испания)

    - Паспорт (Испания)
    - Уникальный номер налогоплательщика (Испания)
- Персональные данные (Турция):
    - Водительское удостоверение (Турция)
    - Идентификационный номер иностранца (Турция)
    - Удостоверение личности (Турция)
    - Номер регистрации социального страхования (4/a SSK) (Турция)
    - Паспорт (Турция)
    - Идентификационный номер налогоплательщика (Турция)
- Персональные данные (Великобритания):
    - Водительское удостоверение (Великобритания)
    - Номер социального страхования (Великобритания)
    - Паспорт (Великобритания)
    - Удостоверение на проживание (Великобритания)
    - Уникальный номер налогоплательщика (UTR) (Великобритания)
- Персональные данные (США):
    - Водительское удостоверение (США)
    - Индивидуальный идентификационный номер налогоплательщика (ITIN) (США)
    - Паспорт (США)
    - Номер социального страхования (SSN) (США)

Начало использования Data Discovery

Приступить к использованию функции Data Discovery можно при первом запуске Консоли управления Kaspersky Security Center Cloud Console или после обновления Kaspersky Security Center Cloud Console до новой версии. Если вы не включили использование Data Discovery во время первоначальной или дополнительной настройки Kaspersky Security Center Cloud Console, можно сделать это, как описано в данном разделе.

Чтобы начать использовать Data Discovery:

1. Откройте Консоль управления Kaspersky Security Center Cloud Console.
2. Выполните любое из следующих действий:
   - В разделе **Панель информации** перейдите на вкладку **Начало работы**.
   - В разделе **Панель информации** перейдите на вкладку **Мониторинг**.
   - В разделе **Параметры** перейдите по ссылке **Параметры** в разделе **Использование Data Discovery для Microsoft 365**.

     Откроется страница **Data Discovery**.
3. Нажмите **Включить Data Discovery**.

   Откроется окно **Соглашение о Data Discovery**.
4. Ознакомьтесь с Соглашением об ограничении ответственности, установите флажок под текстом соглашения и, в случае согласия с его условиями, нажмите на кнопку **Я принимаю условия**.

   При нажатии на кнопку **Я отказываюсь** вы не сможете пользоваться Data Discovery.

Data Discovery включен.

Затем необходимо подключить организацию Microsoft 365 к рабочей области. После этого появится возможность просматривать информацию об обнаружениях.

Позже вы можете выключить эту функцию, если не захотите ее использовать.

Принятие условий Соглашения о Data Discovery

Чтобы принять условия Соглашения о Data Discovery:

1. Откройте Консоль управления Kaspersky Security Center Cloud Console.
2. Выполните любое из следующих действий:
   - (Если виджет **Обнаружения компонента Data Discovery** был добавлен на панель мониторинга) В разделе **Мониторинг → Панель мониторинга** в блоке **Обнаружения компонента Data Discovery** нажмите на кнопку **Включить Data Discovery**.
   - В разделе **Службы → Data Discovery** нажмите на кнопку **Включить Data Discovery**.

   Откроется окно **Соглашение о Data Discovery**.
3. Ознакомьтесь с Соглашением, установите флажок под текстом соглашения и, в случае согласия с его условиями, нажмите на кнопку **Я принимаю условия**.

   > При нажатии на кнопку **Я отказываюсь** вы не сможете пользоваться Data Discovery.

Условия Соглашения о Data Discovery приняты.

Kaspersky Security Center Cloud Console предложит вам подключить свою организацию Microsoft 365 к рабочей области.

Подключение организации Microsoft 365 к рабочей области

После того как вы включили использование компонента Data Discovery, необходимо подключить вашу организацию Microsoft 365 к рабочей области Kaspersky Security Center Cloud Console, как описано в этом разделе. После этого вы сможете просматривать обнаружения компонента Data Discovery в Консоли управления.

Чтобы подключить организацию Microsoft 365 к рабочей области:

1. Откройте Консоль управления Kaspersky Security Center Cloud Console.
2. Выполните любое из следующих действий:
   - В разделе **Панель информации** перейдите на вкладку **Начало работы** и нажмите на кнопку **Подключить организацию Microsoft 365**.
   - В разделе **Панель информации** перейдите на вкладку **Мониторинг**, а затем нажмите на кнопку **Подключить организацию Microsoft 365** или перейдите по ссылке **Подключить организацию Microsoft 365**.

   Вы будете перенаправлены на сайт Microsoft Online.
3. Укажите учетную запись глобального администратора Microsoft 365 и примите предоставление запрошенных разрешений.

   Указанная вами учетная запись глобального администратора должна принадлежать той организации Microsoft 365, о которой вы хотите просмотреть информацию. Обратите внимание, что Kaspersky Security Center Cloud Console не хранит учетные данные глобального администратора и использует только полученное согласие.

   Вы вернетесь в Консоль управления Kaspersky Security Center Cloud Console.

После проверки и подтверждения указанных учетных данных ваша организация Microsoft 365 будет подключена к рабочей области Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console запустит первую проверку файлов, находящихся в облачных хранилищах Microsoft 365.

После завершения проверки вы сможете просмотреть обнаружения в виджете и таблице Data Discovery.

Просмотр информации об обнаружениях Data Discovery

Вы можете просмотреть информацию об обнаружениях Data Discovery в виджете и в таблице. Виджет показывает до 5 обнаруженных файлов, а таблица – до 1000 обнаружений.

Виджет Data Discovery

Чтобы посмотреть виджет Data Discovery:

1. Откройте Консоль управления Kaspersky Security Center Cloud Console.
2. В разделе **Панель информации** перейдите на вкладку **Мониторинг**.
3. Если компонент Data Discovery выключен, включите его.

   Виджет Data Discovery отображает до 10 обнаруженных файлов.
4. Установите или снимите флажки **Закрытый**, **Корпоративный** и **Открытый**, чтобы просмотреть до 10 обнаруженных файлов, доступных выбранной аудитории (внутри или за пределами компании).
5. Щелкните ссылку в столбце **Категории данных** или **Имя файла**, чтобы просмотреть подробную информацию об обнаруженном файле.

В виджете отображаются запрашиваемые данные.

Из виджета можно перейти к таблице с обнаружениями компонента Data Discovery.

Таблица Data Discovery

Чтобы просмотреть таблицу с обнаружениями Data Discovery:

1. Откройте Консоль управления Kaspersky Security Center Cloud Console.
2. Выполните любое из следующих действий:
   - В разделе **Панель информации** откройте вкладку **Мониторинг**, а затем перейдите по ссылке **Перейти к списку обнаружений** в виджете Data Discovery.
   - Выберите раздел **Управление безопасностью** → **Data Discovery**.
3. Если компонент Data Discovery выключен, включите его.

   В таблице отображается до 1000 обнаруженных файлов.
4. Отфильтруйте отображаемые записи:
   a. По умолчанию отображается быстрый фильтр. Вы можете отфильтровать отображаемые записи по сервису Microsoft 365, в котором хранятся обнаруженные файлы.
   b. Выберите **Расширенный фильтр**, чтобы использовать расширенный фильтр.
   c. В раскрывающихся списках выберите требуемые значения:
      - **Дата последнего изменения** – период, за который были обнаружены файлы.
      - **Категории данных** – категории важной информации, обнаруженной в файлах.

- **Тип доступа** – аудитория, которой доступны файлы (внутри или за пределами компании).
- **Автор последнего изменения** – если вы выберете значение **Пользовательский**, откроется окно **Автор последнего изменения**. Укажите фрагмент текста, по которому нужно найти учетные записи пользователей, вносивших последние изменения в обнаруженные файлы.
- **Название сервиса** – сервис Microsoft 365, в котором хранятся обнаруженные файлы.

d. Выберите **Экспресс-фильтр**, чтобы вернуться к быстрому фильтру.

5. Щелкните ссылку в столбце **Имя файла** или **Категории данных**, чтобы просмотреть подробную информацию об обнаруженном файле.

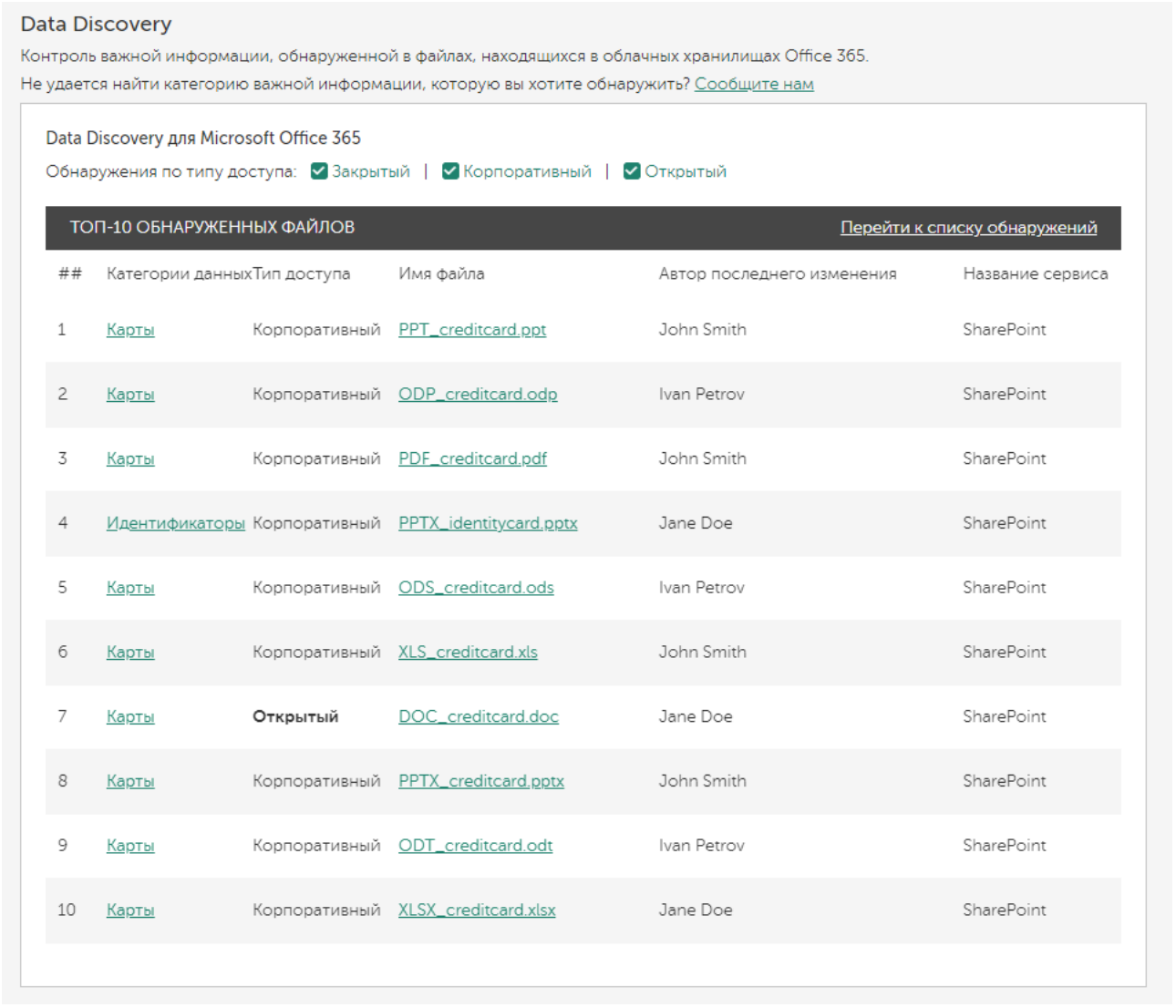
В таблице отображаются запрашиваемые данные.

Из отображаемой таблицы можно экспортировать информацию обо всех текущих обнаружениях в файл CSV.

Пример анализа обнаружения Data Discovery

В этом разделе приведен пример обнаружения Data Discovery, а также описан его анализ и обработка.

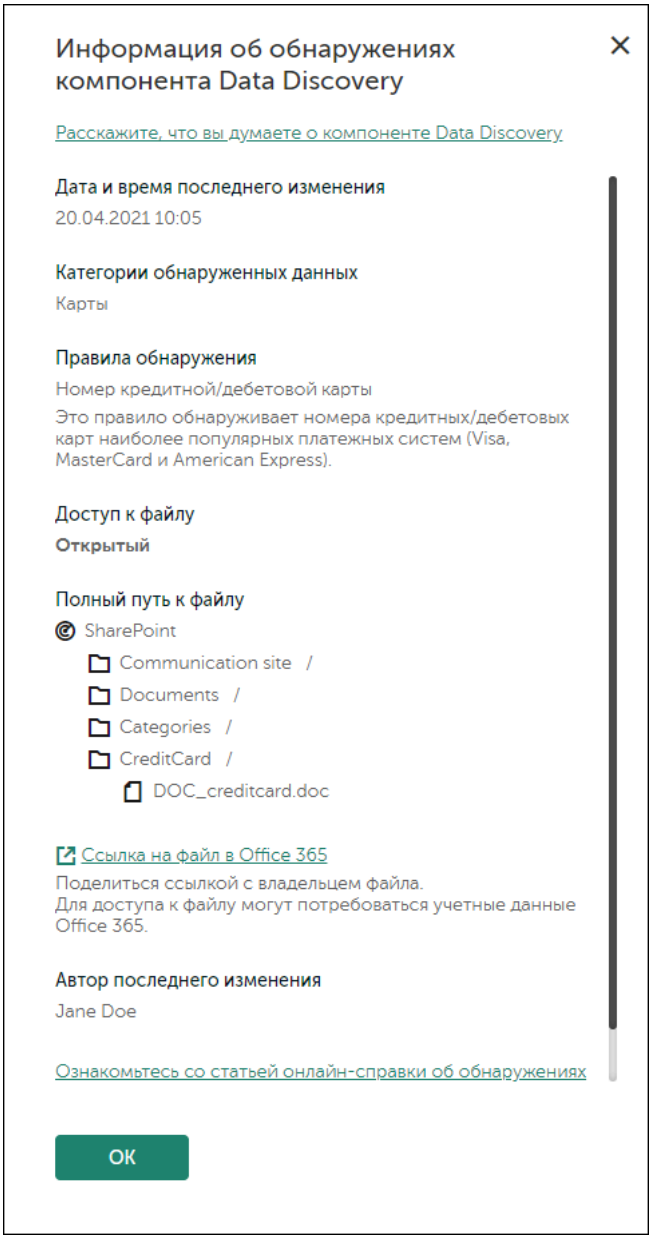
Предположим, вы открыли виджет Data Discovery (см. рис. ниже) и видите файл, доступный для всех (в столбце **Тип доступа** отображается значение **Открытый**).



Виджет Data Discovery с общедоступным файлом

Значение в столбце **Категории данных** показывает, что файл содержит данные кредитной карты. Значение в столбце **Автор последнего изменения** чаще всего показывает, какой пользователь настроил доступность файла.

Перейдя по ссылке в столбце **Категории данных** или **Имя файла**, можно просмотреть подробную информацию об обнаруженном файле (см. рис. ниже).

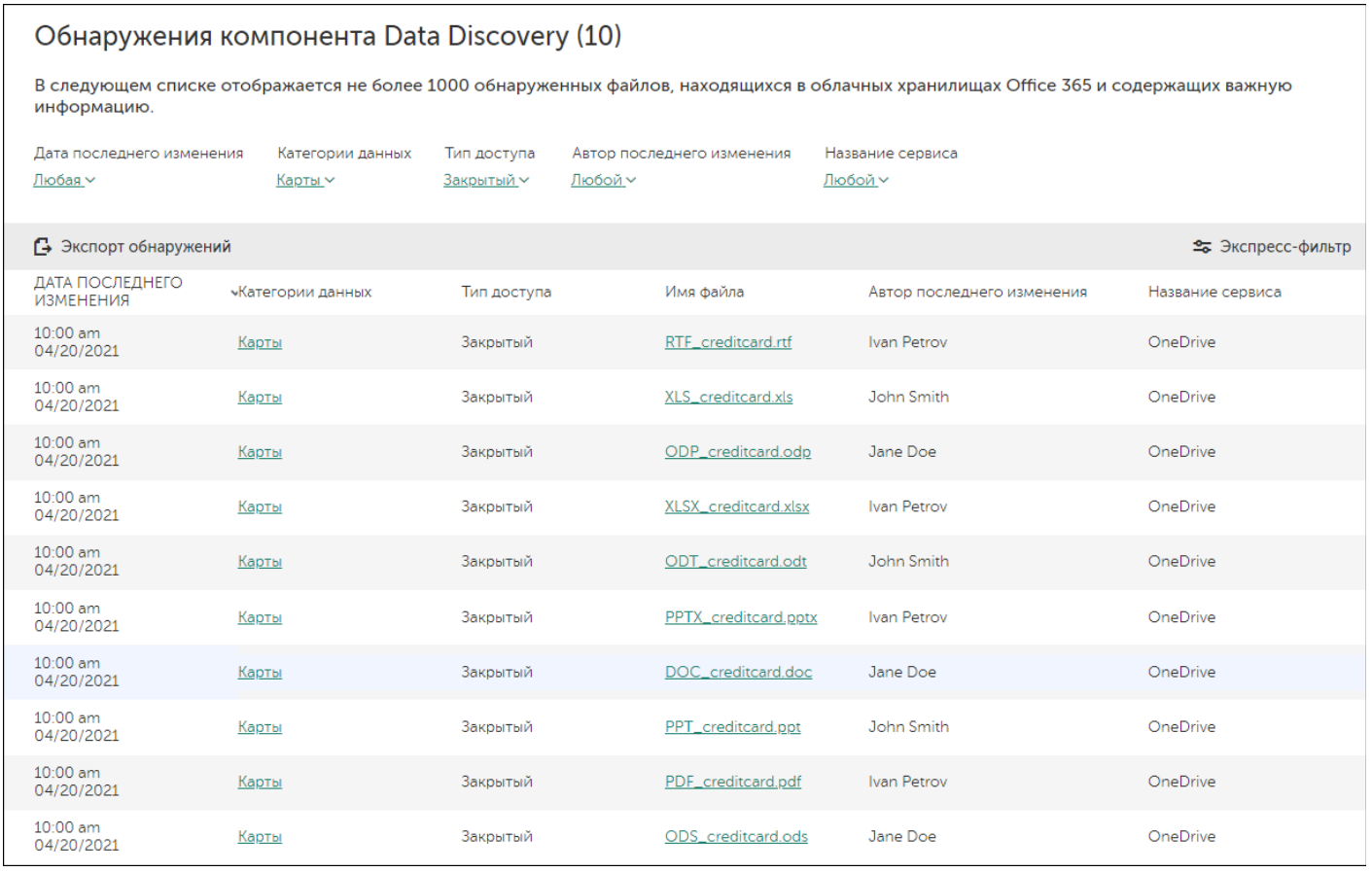


Информация об обнаружении Data Discovery

Вы можете скопировать либо прямую ссылку на файл (**Ссылка на файл в Microsoft 365**), либо структуру пути к нему (в разделе **Полный путь к файлу**).

Затем вы можете напрямую обратиться к пользователю, показать ему файл и объяснить, что предоставление общего доступа к файлу с личными данными может привести к утечке данных. Можно попросить пользователя сократить аудиторию, которой доступен файл, до самого пользователя.

После того как пользователь последует вашему совету, вы можете открыть таблицу Data Discovery, применить фильтры (при необходимости) и увидеть тот же документ, который теперь доступен только его владельцу (см. рис. ниже).



Обнаружения компонента Data Discovery (10)

В следующем списке отображается не более 1000 обнаруженных файлов, находящихся в облачных хранилищах Office 365 и содержащих важную информацию.

Дата последнего изменения: Любая | Категории данных: Карты | Тип доступа: Закрытый | Автор последнего изменения: Любой | Название сервиса: Любой

Экспорт обнаружений | Экспресс-фильтр

ДАТА ПОСЛЕДНЕГО ИЗМЕНЕНИЯ	Категории данных	Тип доступа	Имя файла	Автор последнего изменения	Название сервиса
10:00 am 04/20/2021	Карты	Закрытый	RTF_creditcard.rtf	Ivan Petrov	OneDrive
10:00 am 04/20/2021	Карты	Закрытый	XLS_creditcard.xls	John Smith	OneDrive
10:00 am 04/20/2021	Карты	Закрытый	ODP_creditcard.odp	Jane Doe	OneDrive
10:00 am 04/20/2021	Карты	Закрытый	XLSX_creditcard.xlsx	Ivan Petrov	OneDrive
10:00 am 04/20/2021	Карты	Закрытый	ODT_creditcard.odt	John Smith	OneDrive
10:00 am 04/20/2021	Карты	Закрытый	PPTX_creditcard.pptx	Ivan Petrov	OneDrive
10:00 am 04/20/2021	Карты	Закрытый	DOC_creditcard.doc	Jane Doe	OneDrive
10:00 am 04/20/2021	Карты	Закрытый	PPT_creditcard.ppt	John Smith	OneDrive
10:00 am 04/20/2021	Карты	Закрытый	PDF_creditcard.pdf	Ivan Petrov	OneDrive
10:00 am 04/20/2021	Карты	Закрытый	ODS_creditcard.ods	Jane Doe	OneDrive

Таблица Data Discovery с примененными фильтрами

Экспорт информации об обнаружениях Data Discovery

Из таблицы обнаружений Data Discovery можно экспортировать информацию обо всех текущих обнаружениях в файл CSV. Например, файл с обнаружениями можно использовать для подготовки отчета для руководства.

Чтобы экспортировать информацию об обнаружениях Data Discovery:

1. Перейдите к таблице с обнаружениями Data Discovery.
2. Нажмите на кнопку **Экспорт обнаружений**.

   Откроется окно **Экспортировать обнаружения Data Discovery**.
3. Нажмите на кнопку **Экспорт** для подтверждения.

Файл с обнаружениями Data Discovery будет создан и автоматически загружен. Файл содержит те же столбцы, что и таблица с обнаружениями.

Выключение Data Discovery

Если вы хотите прекратить использование компонента Data Discovery, вы можете выключить его, как описано в этом разделе.

Чтобы выключить компонент Data Discovery:

1. Откройте Консоль управления Kaspersky Security Center Cloud Console.
2. Выберите раздел **Параметры**.

   Откроется страница **Общие параметры Kaspersky Security Center Cloud Console**.
3. Перейдите по ссылке **Параметры** в разделе **Использование Data Discovery для Microsoft 365**.

   Откроется страница **Data Discovery**.
4. Нажмите на кнопку **Выключить Data Discovery**.
5. В открывшемся окне подтверждения нажмите на кнопку **Выключить**.

Data Discovery выключен.

В дальнейшем можно снова включить этот компонент.

Обнаружение сетевых устройств и создание групп администрирования

В этом разделе описаны поиск устройств и опрос сети, а также создание групп администрирования для этих устройств.

Kaspersky Security Center Cloud Console позволяет искать устройства на основании заданных критериев. Вы можете сохранить результаты поиска в текстовый файл.

Функция поиска позволяет находить следующие устройства:

- управляемые устройства в группах администрирования Сервера администрирования Kaspersky Security Center Cloud Console и его подчиненных Серверов;
- нераспределенные устройства под управлением Сервера администрирования Kaspersky Security Center Cloud Console и его подчиненных Серверов.

Сценарий: обнаружение сетевых устройств

Вам нужно выполнить поиск устройств перед первоначальным развертыванием 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.

После завершения сценария обнаружение устройств настроено и будет выполняться в соответствии с указанным расписанием.

Предварительные требования

В Kaspersky Security Center Cloud Console обнаружение устройств выполняется точками распространения. Прежде чем начать, сделайте следующее:

- Решите, какое устройство будет выполнять роль точки распространения.
- Установите Агент администрирования на выбранное устройство.
- Вручную назначьте устройство точкой распространения.

Этапы

Сценарий состоит из следующих этапов:

1. **Выбор типа обнаружения**

   Определите, какой тип обнаружения устройств вы хотите регулярно использовать.

2. **Настройка опросов**

   В свойствах каждой точки распространения включите и настройте выбранные типы сетевого опроса: опрос сети Windows, опрос контроллеров домена или опрос IP-диапазонов. Убедитесь, что расписание опроса соответствует нуждам вашей организации.

   Если сетевые устройства включены в домен, рекомендуется использовать опрос контроллеров домена.

3. **Задание правил для добавления обнаруженных устройств в группы администрирования (если требуется)**

   Если в сети появились новые устройства, они будут обнаружены при опросах сети. Такие устройства 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 шаг, 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.

Когда опрос завершен, вы можете просмотреть список новых обнаруженных устройств, распределенных в соответствии с заданными правилами. Если правила не заданы, устройства остаются в группе **Нераспределенные устройства**.

Опрос сети

Информацию о структуре сети и входящих в ее состав устройствах Сервер администрирования Kaspersky Security Center Cloud Console получает в ходе регулярных опросов сети Windows, IP-диапазонов и контроллеров домена Microsoft Active Directory и контроллеров домена Samba. Для контроллеров домена Samba, в качестве контроллеров домена Active Directory используется Samba 4. Опрос сети можно запустить либо вручную, либо автоматически по расписанию.

В зависимости от результатов опроса Kaspersky Security Center Cloud Console обновляет список нераспределенных устройств. Можно также настроить правила автоматического перемещения новых обнаруженных устройств в определенные группы администрирования.

Kaspersky Security Center Cloud Console использует следующие способы опроса сети:

- *Опрос IP-диапазонов*. Kaspersky Security Center Cloud Console опрашивает сформированные IP-диапазоны с помощью ICMP-пакетов и получает полную информацию об устройствах, входящих в IP-диапазоны.

- *Опрос сети Windows*. Существуют два вида опроса сети Windows: быстрый опрос и полный опрос. При быстром опросе Kaspersky Security Center Cloud Console получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети. Во время полного опроса с каждого клиентского устройства запрашивается следующая информация: имя операционной системы, IP-адрес, DNS-имя, NetBIOS-имя.

- *Опрос контроллеров домена*. В базу данных Kaspersky Security Center Cloud Console записывается информация о структуре групп Active Directory, а также информация о DNS-именах устройств, входящих в группы Active Directory.

Результаты опроса отображаются в разделе **Обнаружение устройств и развертывание → Обнаружение устройств** отдельно для *опроса Windows-сети* и *опроса контроллеров домена*.

Результаты опроса для *опроса IP-диапазонов* отображаются в разделе **Обнаружение устройств и развертывание → Нераспределенные устройства**.

Одно и то же устройство может входить в результаты нескольких способов опроса. Если устройство обнаружено в домене HQ и его IP-адрес 192.168.0.1, устройство будет отображаться в разделе **Windows-домены** и в разделе **Нераспределенные устройства**. Можно настроить параметры опроса сети для каждого способа опроса. Например, может потребоваться изменить расписание опроса или указать, нужно опрашивать весь лес Active Directory или только определенный домен.

Опрос сети Windows

Об опросе сети Windows

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

- имя операционной системы;

- IP-адрес;

- DNS-имя;

- NetBIOS-имя.

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

- наличие открытых портов UDP 137/138, TCP 139;

- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на точке распространения;

- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на клиентском устройстве:
  - наличие хотя бы одного устройства, если количество сетевых устройств не превышает 32;
  - наличие как минимум одного устройства на каждые 32 сетевых устройства.

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

Просмотр и изменение параметров опроса сети Windows

Чтобы изменить параметры опроса сети Windows:

1. В главном окне 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, которую вы хотите использовать для опроса сети.

   Откроется окно свойств точки распространения.

4. Выберите раздел **Опрос Windows-доменов**.

5. Включите или выключите опрос Windows сети, используя переключатель **Разрешить опрос сети**.

6. Настройте расписание быстрого опроса и полного опроса.

   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.

7. Сохраните параметры опроса сети Windows.

Параметры сохранены и применены ко всем Windows-доменам и рабочим группам.

Опрос контроллеров домена

Kaspersky Security Center Cloud Console поддерживает опрос контроллеров домена только с помощью точек распространения. Вы можете настроить опрос следующих типов контроллеров домена:

- Microsoft Active Directory.
- Samba.
- FreeIPA.
- ALD Pro.

Kaspersky Security Center Cloud Console опрашивать контроллер домена Samba только с помощью точки распространения с операционной системой Linux. Для контроллеров домена Samba, в качестве контроллеров домена Active Directory используется Samba 4.

При опросе контроллеров домена точка распространения получает информацию о структуре домена, учетных записях пользователей, группах безопасности и о DNS-именах устройств, входящих в домен. Опрос контроллеров домена выполняется по заданному вами расписанию.

Предварительные требования

Перед опросом контроллеров домена убедитесь, что включены следующие протоколы:

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

Убедитесь, что на устройстве контроллеров домена доступны следующие порты:

- 389 для SASL.
- 636 для TLS.

Опрос контроллеров домена с помощью 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 контроллера домена для опроса.
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 Cloud Console.

Просмотр результатов опроса контроллеров домена

Чтобы просмотреть результаты опроса контроллеров домена:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Контроллеры доменов**.

   Отобразится список обнаруженных организационных подразделений.

2. Выберите организационное подразделение и нажмите на кнопку **Устройства**.

   Отобразится список устройств организационного подразделения.

Вы можете выполнить поиск устройств в списке и фильтровать результаты.

Опрос IP-диапазонов

Kaspersky Security Center Cloud Console пытается выполнить обратное преобразование имен: для каждого IP-адреса из указанного диапазона выполнить преобразование в DNS-имя с помощью стандартных DNS-запросов. Если данная операция завершается успешно, сервер отправляет запрос `ICMP ECHO REQUEST` (аналог команды ping) на полученное имя. Если устройство отвечает, информация об этом устройстве добавляется в базу данных Kaspersky Security Center Cloud Console. 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. В сетях, в которых используется Active Directory, такая зона поддерживается автоматически. Но в таких сетях опрос IP-подсети не предоставляет дополнительной информации, помимо информации из опроса Active Directory. Кроме того, администраторы малых сетей часто не выполняют настройку зон обратного просмотра DNS, поскольку это не является необходимым для работы многих сетевых служб. Из-за этих причин опрос IP-подсети по умолчанию отключен.

Исходно Kaspersky Security Center Cloud Console получает IP-диапазоны для опроса из сетевых параметров устройства, выполняющего роль точки распространения, которое используется для опроса сети. Если адрес устройства 192.168.0.1, а маска подсети – 255.255.255.0, Kaspersky Security Center Cloud Console автоматически включит сеть 192.168.0.0/24 в список адресов для опроса. Kaspersky Security Center Cloud Console выполнит опрос всех адресов от 192.168.0.1 до 192.168.0.254.

Не рекомендуется использовать опрос IP-диапазонов, если вы используете опрос сети Windows и/или опрос Active Directory.

Просмотр и изменение параметров опроса IP-диапазонов

Чтобы просмотреть и изменить параметры опроса IP-диапазонов:

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, которую вы хотите использовать для опроса сети.

   Откроется окно свойств точки распространения.

4. Выберите раздел **Опрос IP-диапазонов**.

5. Включите или выключите опрос IP-диапазонов, используя переключатель **Разрешить опрос диапазона**.

6. Настройте расписание опроса. По умолчанию опрос IP-диапазонов запускается каждые 420 минут (семь часов).

7. Если необходимо, добавьте или измените IP-диапазоны для опроса.

   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.

8. Нажмите на кнопку **OK**.

Параметры будут сохранены и применены ко всем IP-диапазонам.

Настройка контроллеров домена Samba

Kaspersky Security Center Cloud Console 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 Cloud Console и контроллера домена Samba.

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

1. Выполните 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.

Добавление и изменение IP-диапазона

Исходно Kaspersky Security Center Cloud Console получает IP-диапазоны для опроса из сетевых параметров устройства, выполняющего роль точки распространения, которое используется для опроса сети. Если адрес устройства 192.168.0.1, а маска подсети – 255.255.255.0, Kaspersky Security Center Cloud Console автоматически включит сеть 192.168.0.0/24 в список адресов для опроса. Kaspersky Security Center Cloud Console 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.

Чтобы добавить новый IP-диапазон:

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, которую вы хотите использовать для опроса сети.

   Откроется окно свойств точки распространения.

4. Выберите раздел **Опрос IP-диапазонов**.

5. Чтобы добавить IP-диапазон, нажмите на кнопку **Добавить**.

6. В открывшемся окне настройте следующие параметры:

   - **Имя**

     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. Вы можете добавить столько подсетей, сколько необходимо. Именованные IP-диапазоны не должны пересекаться, но на неименованные подсети внутри IP-диапазонов это ограничение не распространяется.

   - **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.

7. Нажмите на кнопку **OK**.

IP-диапазон добавлен в список IP-диапазонов.

После завершения опроса вы можете просмотреть список обнаруженных устройств, нажав на кнопку **Устройства**. По умолчанию срок действия результатов опроса составляет 24 часа, он равен времени действия IP-адреса.

Настройка точек распространения и шлюзов соединений

Структура групп администрирования в Kaspersky Security Center Cloud Console выполняет следующие функции:

- Задание области действия политик.

  Существует альтернативный способ применения нужных наборов параметров на устройствах с помощью *профилей политик*. В этом случае область применения политик задается с помощью тегов, местоположения устройств в подразделениях Active Directory, членства в группах безопасности Active Directory и прочего.

- 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 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.

Расчет количества и конфигурации точек распространения

Чем больше клиентских устройств содержит сеть, тем больше требуется точек распространения. Используйте таблицу ниже, чтобы рассчитать количество точек распространения, необходимое для вашей сети.

Убедитесь, что устройства, которые вы хотите использовать в качестве точек 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 недоступна, рассмотрите возможность обновления баз, модулей приложений и приложений "Лаборатории Касперского" вручную или напрямую с серверов обновлений "Лаборатории Касперского".

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.

- Построение структуры групп администрирования, не отражающей топологию сети. В этом случае следует 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.

Назначение точек распространения вручную

Kaspersky Security Center Cloud Console позволяет вручную назначать устройства точками распространения. Рекомендуется рассчитать количество точек распространения и их конфигурацию, необходимые для вашей сети.

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

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

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

Чтобы вручную назначить устройство точкой распространения:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.

3. Нажмите на кнопку **Назначить**.

4. 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.

5. Выберите группу администрирования, которую вы хотите включить в область действия выбранной точки распространения.

6. Нажмите на кнопку **Добавить**.

   Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.

7. Выберите в списке добавленную точку распространения, чтобы открыть окно ее свойств.

8. В окне свойств настройте параметры точки распространения:

   - В разделе **Общие** укажите параметры взаимодействия точки распространения с клиентскими устройствами:

     - **SSL-порт**

       Номер SSL-порта, по которому осуществляется защищенное подключение клиентских устройств к точке распространения с использованием протокола SSL.

       По умолчанию номер порта – 13000.

- **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 Cloud Console автоматически назначает уникальный IP-адрес многоадресной рассылки в заданном диапазоне.

- **Номер порта IP-рассылки**

  Номер порта многоадресной рассылки.

  Номер порта по умолчанию – 15001. Если в качестве точки распространения указано устройство, на котором установлен Сервер администрирования, то для подключения с использованием SSL-протокола по умолчанию используется порт 13001.

- **Адрес точки распространения для удаленных устройств**

  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 Cloud Console точка распространения может работать как push-сервер для устройств на базе Windows и Linux, управляемых Агентом 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 push-сервер на каждой из 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 область, на которую точка распространения распространяет обновления (группы администрирования и/или сетевое местоположение).

  Если вы хотите указать группу администрирования, нажмите на кнопку **Добавить группу**. В открывшейся правой панели выберите группу администрирования из раскрывающегося списка и нажмите на кнопку **Добавить**.

  Если вы хотите указать подсеть, нажмите на кнопку **Добавить подсеть**. В открывшейся правой панели нажмите на кнопку **Добавить** и укажите имя подсети.

  Для устройств с операционной системой Windows отображается переключатель **Автоматически назначать точки распространения в рамках данного сетевого местоположения**. Определение сетевого местоположения недоступно для устройств под управлением других операционных систем.

- В разделе **Источник обновлений** можно выбрать источник обновлений для точки распространения.

- Если ваши точки распространения используют прокси-сервер для подключения к интернету, в разделе **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.

    > Такая возможность не поддерживается для точек распространения под управлением Linux или macOS.

    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 параметр **Я принимаю условия использования Kaspersky Security Network** включен 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.

  - **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** вы можете настроить точку распространения для работы в роли шлюза для соединения между экземплярами Агента администрирования и Сервером администрирования, если прямое соединение не может быть установлено из-за организации вашей сети. Для этого включите переключатель **Шлюз соединения**.

  По умолчанию параметр выключен.

  При подключении мобильных устройств к Серверу администрирования через точку распространения, выполняющую роль шлюза соединения, вы можете включить следующие параметры:

  - **Открыть порт для мобильных устройств (SSL-аутентификация только Сервера администрирования)**

    Включите этот параметр, если требуется, чтобы шлюз соединения открывал порт для мобильных устройств, и укажите номер порта, который мобильные устройства будут использовать для подключения к точке распространения. По умолчанию установлен порт 13292. Мобильное устройство проверит сертификат Сервера администрирования. При установке соединения только Сервер администрирования выполняет аутентификацию.

  - **Открыть порт для мобильных устройств (двусторонняя SSL-аутентификация)**

    Включите этот параметр, если требуется, чтобы шлюз соединения открывал порт, который будет использоваться для двусторонней аутентификации Сервера администрирования и мобильных устройств. Мобильное устройство проверит сертификат Сервера администрирования, а Сервер администрирования проверит сертификат мобильного устройства. Задайте следующие параметры:

    - Номер порта, который мобильные устройства будут использовать для подключения к точке распространения. По умолчанию установлен порт 13293.

    - Имена DNS-доменов шлюза соединения, которые будут использоваться мобильными устройствами. Разделяйте имена доменов запятыми. Указанные имена доменов будут включены в сертификат точки распространения. Если имена доменов, используемые мобильными устройствами, не совпадают с общим именем в сертификате точки распространения, мобильные устройства не подключаются к точке распространения.

      Имя DNS-домена по умолчанию – это полное имя домена шлюза соединения.

  В обоих случаях сертификаты проверяются во время установки TLS-сеанса только на точке распространения. Сертификаты не пересылаются на проверку Сервером администрирования. После установки TLS-сеанса с мобильным устройством точка распространения использует сертификат Сервера администрирования для создания туннеля для синхронизации между мобильным устройством и Сервером администрирования. Если вы откроете порт для двусторонней SSL-аутентификации, единственный способ распространить сертификат мобильного устройства – это с помощью установочного пакета.

- Настройте опрос доменов Windows, контроллеров домена и IP-диапазонов точкой распространения:

  - **Опрос Windows-доменов**

    Вы можете включить обнаружение устройств для Windows-доменов, включив переключатель **Разрешить опрос сети** и нажав на кнопку **Настроить расписание полного опроса**, чтобы задать расписание для обнаружения.

В открывшемся окне настройте следующие параметры:

- **Запуск по расписанию**

  Вы можете выбрать один из следующих вариантов расписания:

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

  - **По дням недели**

    Опрос выполняется регулярно, в указанные дни недели, в указанное время. По умолчанию опрос запускается каждую пятницу в 18:00:00.

  - **Ежемесячно в выбранный день**

    Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время. По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **Интервал запуска (сут)**

  Укажите значение N (для минут или дней).

  Поле отображается, если вы выбрали вариант расписания **Каждые N дней** или **Каждые N минут**.

- **Начиная с момента**

  Укажите начало первого опроса.

  Поле отображается, если вы выбрали вариант расписания **Каждые N дней** или **Каждые N минут**.

- **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.

  По умолчанию этот параметр выключен. Это означает, что Сервер администрирования ждет следующего планового опроса.

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

Раздел отображается только для точек распространения с операционной системой Windows.

- **Опрос контроллеров домена**

Вы можете включить опрос Active Directory и задать расписание опроса.

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

- **Опросить текущий домен Active Directory**.
- **Опросить лес доменов Active Directory**.
- **Опросить указанные домены Active Directory**. Если вы выбрали этот вариант, добавьте один или несколько доменов Active Directory в список.

Если вы используете точку распространения с операционной системой Linux с установленным Агентом администрирования версии 15, вы можете опрашивать только те домены Active Directory, для которых вы указываете адрес и учетные данные пользователя. Опрос текущего домена Active Directory и леса доменов Active Directory недоступен.

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**

- **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.

- В разделе **Статистика** вы можете просмотреть статистику по загрузке антивирусных баз на устройство или статистику по установке пакетов на устройство.

9. Нажмите на кнопку **OK**.

В результате выбранные устройства будут выполнять роль точек распространения.

Изменение списка точек распространения для группы администрирования

Вы можете просмотреть список точек распространения, назначенных для определенной группы администрирования, и изменить список, добавив или удалив точки распространения.

Чтобы просмотреть и изменить список точек распространения для группы администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами → Активы (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.

   В результате отображается 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. Добавьте новые точки распространения для группы администрирования с помощью кнопки **Назначить** или удалите назначенные точки распространения с помощью кнопки **Отменить назначение**.

   После того как вы нажмете на кнопку **Отменить назначение** устройство будет удалено из группы администрирования и перестанет выполнять роль точки распространения.

В зависимости от изменений, точки распространения добавляются в список или существующие точки распространения удаляются из списка.

Использование точки распространения в качестве извещающего сервера

В Kaspersky Security Center Cloud Console точка распространения может работать как push-сервер для устройств на базе Windows и Linux, управляемых Агентом 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 push-сервер на каждой из них. В этом случае Сервер администрирования распределяет нагрузку между точками распространения.

Вы можете использовать точки распространения в качестве push-серверов, чтобы установить постоянное соединение 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 отправлять пакеты на UDP-порт Агента администрирования.

Чтобы использовать точку распространения в качестве push-сервера:

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 точку распространения, которую вы хотите использовать в качестве push-сервера.

4. В списке свойств выбранной точки распространения перейдите в раздел **Общие** и включите параметр **Включено**.

   Поле ввода **Порт push-сервера** станет доступным.

5. В поле ввода **Порт push-сервера** укажите порт точки распространения, который клиентские устройства будут использовать для подключения. По умолчанию номер порта – 13295.

   > В правилах сетевого экрана вам нужно разрешить исходящие сетевые соединения между управляемыми устройствами и портом push-сервера.

6. Нажмите **ОК**, чтобы закрыть окно свойств точки распространения, а затем нажмите **Сохранить**, чтобы применить изменения.

   После включения параметра **Включено** параметр **Не разрывать соединение с Сервером администрирования** автоматически включится на точке распространения, которая используется в качестве push-сервера. Этот параметр позволяет установить предварительное соединение между Агентом администрирования и Сервером администрирования.

7. Откройте окно Параметры политики Агента администрирования.

8. Перейдите в раздел **Подключения** → **Сеть** и включите параметр **Использовать точку распространения для принудительного подключения к Серверу администрирования**. Установите замок для этого параметра.

9. В подразделе **Сеть** вы также можете отключить параметр **Использовать UDP-порт**. После настройки push-сервер перестанет отправлять пакеты через UDP-порт и будет поддерживать непрерывное соединение между управляемым устройством и Сервером администрирования.

10. Нажмите на кнопку **OK**, чтобы закрыть окно.

Точка распространения начинает выполнять роль push-сервера. Теперь он может отправлять push-уведомления на клиентские устройства.

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 Cloud Console не обеспечивает постоянного соединения между управляемыми устройствами и Сервером администрирования. Агенты администрирования на управляемых устройствах периодически устанавливают соединение и синхронизируются с Сервером администрирования. Продолжительность периода такой синхронизации задается в политике Агента администрирования. Если требуется предварительная синхронизация, Сервер администрирования (или точка распространения, если она используется) отправляет подписанный сетевой пакет по IPv4-сети 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 остановка локальных задач, получение статистики по управляемому приложению или создание туннеля. Чтобы решить эту проблему, если вы не используете push-серверы, вы можете использовать параметр **Не разрывать соединение с Сервером администрирования**, который обеспечивает постоянное соединение между управляемым устройством и Сервером администрирования.

Чтобы проверить постоянное соединение управляемого устройства с Сервером администрирования:

1. Выполните одно из следующих действий:

   - Если управляемое устройство обращается к Серверу администрирования напрямую (то есть не через точку распространения), в главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)** и нажмите на имя устройства, с которым вы хотите обеспечить постоянную связь.

     Откроется окно свойств управляемого устройства.

   - Если управляемое устройство обращается к Серверу администрирования через точку распространения, работающую в режиме шлюза, а не напрямую:

     a. Откройте окно свойств Сервера администрирования, нажав на имя Сервера администрирования в главном меню.

        Вы также можете перейти к свойствам нужного Сервера администрирования из панели навигации. Для этого в главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Settings**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**. В открывшейся панели наведите курсор мыши на название нужного Сервера администрирования и нажмите на значок параметров (⚙).

b. На вкладке **Общие** выберите раздел **Точки распространения**.

c. Выберите имя нужной точки распространения из списка точек распространения.

Откроется окно свойств выбранной точки распространения.

2. В разделе **Общие** открывшегося окна свойств выберите 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.

Создание групп администрирования

Исходно иерархия групп администрирования содержит только группу администрирования **Управляемые устройства**. При создании иерархии групп администрирования в состав группы **Управляемые устройства** можно включать устройства и виртуальные машины и добавлять вложенные группы. Для каждой группы администрирования окно свойств содержит информацию о политиках, задачах и устройствах, относящихся к группе.

Чтобы создать группу администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами → Иерархия групп**.
2. Установите флажок напротив группы администрирования, для которой вы хотите создать подгруппу.
3. Нажмите на кнопку **Добавить**.
4. Введите имя новой группы администрирования.
5. Нажмите на кнопку **Добавить**.

Новая группа администрирования, с указанным именем, появится в иерархии групп администрирования.

Приложение позволяет создавать структуру групп администрирования на основе структуры Active Directory или структуры доменной сети. Также вы можете создавать структуру групп из текстового файла.

Чтобы создать структуру групп администрирования:

1. В главном окне 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.

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. На вкладке **Общие** укажите следующую информацию:

   - **Имя правила**

     Укажите имя нового правила активации.

     Если вы копируете правило, новое правило получает такое же имя, как и исходное правило, но к нему добавляется индекс в скобках, например: (1).

   - **Группа администрирования**

     Выберите группу администрирования, в которую будут автоматически перемещаться устройства.

   - **Активное правило**

     Если этот параметр включен, правило включено и начинает применяться сразу после сохранения.

     Если этот параметр выключен, правило создается, но оно не включено. Правило не будет работать до тех пор, пока вы не включите этот параметр.

   - **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.

   - **Активное правило**

     Если этот параметр включен, правило включено и начинает применяться сразу после сохранения.

     Если этот параметр выключен, правило создается, но оно не включено. Правило не будет работать до тех пор, пока вы не включите этот параметр.

   - **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.
- Управляемые приложения, установленные на клиентских устройствах, например Агент администрирования или Сервер администрирования.
- Виртуальные машины, которые являются клиентскими устройствами.
- Информация об организационном подразделении Active Directory (OU) с клиентскими устройствами.
- Информация об облачном сегменте с клиентскими устройствами.

Ниже вы можете найти описание того, как указать эту информацию в правиле перемещения устройств.

Если в правиле указано несколько условий, срабатывает логический оператор AND и применяются все условия одновременно. Если вы не выберете какие-либо параметры или оставите некоторые поля пустыми, такие условия не применяются.

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. Также 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 Cloud Console, 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 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 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 16.2** или **Сервер администрирования Kaspersky Security Center 16.2**.

  Если вы не выберете управляемое приложение, условие не будет применяться.

- **Включено**

  Можно выбирать клиентские устройства на основе версии операционной системы. Для этого укажите операционные системы, которые должны быть установлены на клиентских устройствах. В результате правило перемещения устройств применяется к клиентским устройствам с выбранными операционными системами.

Если этот параметр выключен, условие не применяется. По умолчанию параметр выключен.

- **Архитектура операционной системы**

  Можно выбирать клиентские устройства по разрядности операционной системы. В поле **Архитектура операционной системы** можно выбрать одно из следующих значений:

  - **Нет данных**
  - **x86**
  - **AMD64**
  - **IA64**

  Чтобы проверить разрядность операционной системы клиентских устройств:

  1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.
  2. Нажмите на кнопку **Параметры таблицы** справа ( ).
  3. Выберите параметр **Архитектура ОС** и нажмите на кнопку **Сохранить**.

     После этого для каждого управляемого устройства отобразится разрядность 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** → **Активы (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.

- **Включено**

  > 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.

- **Включено**

  > 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 Active Directory, 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 Active Directory.

  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 группы Active Directory, указанной в списке под параметром.

  По умолчанию параметр выключен.

Вкладка Облачные сегменты

На этой вкладке можно указать, что требуется перемещать устройства, которые относятся к определенным облачным сегментам:

- **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**

  При выборе этого параметра правило перемещения устройств применяется не только к выбранному облачному сегменту, но и к дочерним объектам этого 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, обнаруживается ли устройство средствами API:

  - **AWS**. Устройство обнаружено с использованием AWS API, то есть устройство находится в облачном окружении AWS.

  - **Azure**. Устройство обнаружено с использованием Azure API, то есть устройство находится в облачном окружении Azure.

  - **Google Cloud.** Устройство обнаружено с использованием Google API, то есть устройство находится в облачном окружении Google Cloud.

  - **Нет**. Устройство не обнаруживается с помощью AWS, Azure или Google API, то есть оно либо находится вне облачного окружения, либо находится в облачном окружении, но недоступно для поиска с помощью API.

  - **Не задано**. Это условие не применяется.

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 → Активы (Устройства)**.

2. Выберите группу администрирования, в которую вы хотите добавить устройства:

   - Для корневой группы:

     В этом случае вы можете перейти к следующему шагу.

   - Для подгруппы:

     Нажмите на кнопку **Показать иерархию** в верхней части страницы и в открывшемся окне нажмите на имя подгруппы.

Путь к выбранной группе отображается в верхней части страницы. Чтобы перейти к группе администрирования, нажмите на ссылку с названием группы. 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 NetBIOS-имя устройства или DNS-имя.

       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: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

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** → **Активы (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 **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.

2. Если группа администрирования содержит кластеры или массивы серверов, раздел **Активы (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.

Настройка правил хранения для нераспределенных устройств

После того как опрос сети Windows завершен, обнаруженные устройства помещаются в подгруппы группы администрирования Нераспределенные устройства. Эта группа администрирования находится по следующему пути: **Обнаружение устройств и развертывание → Обнаружение устройств → Windows-домены**. Папка **Windows-домены** является родительской группой. Папка содержит дочерние группы, имена которых соответствуют доменам и рабочим группам, обнаруженным во время опроса. Родительская группа может также содержать группы администрирования мобильных устройств. Вы можете настроить правила хранения нераспределенных устройств для родительской группы администрирования и для каждой дочерней группы. Правила хранения не зависят от параметров обнаружения устройств и работают, даже если обнаружение устройств выключено.

Правила хранения устройств не влияют на устройства, на которых один или несколько дисков зашифрованы с помощью полнодискового шифрования. Такие устройства не удаляются автоматически – вы можете удалить их только вручную. Если вам нужно удалить устройство с зашифрованным жестким диском, сначала расшифруйте диск, а затем удалите устройство.

Чтобы настроить правила хранения нераспределенных устройств:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание → Обнаружение устройств → Windows-домены**.

2. Выполните одно из следующих действий:

   - Чтобы настроить параметры родительской группы, нажмите на кнопку **Свойства**.

     Откроется окно свойств Windows-домена.

   - Чтобы настроить параметры дочерней группы, нажмите на ее имя.

     Откроется окно свойств дочерней группы.

3. Настройте следующие параметры:

   - **Удалять устройство из группы, если оно неактивно больше (сут)**

     Если этот параметр включен, вы можете указать временной интервал, после которого устройство автоматически удаляется из группы администрирования. По умолчанию этот параметр распространяется на дочерние группы. Временной интервал, установленный по умолчанию, составляет 7 дней.

     По умолчанию параметр включен.

   - **Наследовать из родительской группы**

     Если этот параметр включен, период хранения для устройств в текущей группе наследуется от родительской группы и не может быть изменен.

     Этот параметр доступен только для дочерних групп.

     По умолчанию параметр включен.

   - **Обеспечить принудительное наследование для дочерних групп**

     Значения параметров будут распределены по дочерним группам, но в свойствах дочерних групп эти параметры недоступны для изменений.

     По умолчанию параметр выключен.

4. Нажмите на кнопку **Принять**.

Ваши изменения сохранены и применены.

Инвентаризация оборудования

Список оборудования (**Операции** → **Хранилища** → **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 Cloud Console 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 **Операции** → **Хранилища** → **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 **OK**.

   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 **Операции** → **Хранилища** → **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.

Настройка защиты сети

В этом разделе содержится информация о настройке вручную политик и задач, о ролях пользователей, о построении структуры групп администрирования и об иерархии задач.

Сценарий: настройка защиты сети

Мастер первоначальной настройки создает политики и задачи с параметрами по умолчанию. Эти параметры могут оказаться не оптимальными или даже запрещенными в организации. Поэтому рекомендуется настроить эти политики и задачи и создать дополнительные политики и задачи, если это необходимо для вашей сети.

Предварительные требования

Убедитесь, что вы успешно завершили основной сценарий первоначальной настройки Kaspersky Security Center Cloud Console, включая мастер первоначальной настройки.

Во время работы мастера первоначальной настройки в корневой группе администрирования **Управляемые устройства** создаются следующие политики и задачи:

- политика Kaspersky Endpoint Security;
- групповая задача обновления Kaspersky Endpoint Security;
- политика Агента администрирования;
- Поиск уязвимостей и требуемых обновлений (задача Агента администрирования).

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. Также вы можете 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.

4. **Оптимизация нагрузки на приложения для защиты конечных точек**

   Чтобы избежать снижение производительности оптимизируйте потребление ресурсов приложениями для защиты конечных точек.

   Подробные инструкции см. в:

   Справка Kaspersky Endpoint Security для Windows

   Справка Kaspersky Endpoint Security для Linux

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. Вы также можете разграничить устройства по использованию этих устройств в Active Directory или по характеристикам аппаратного обеспечения.

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

В этом разделе приведен сценарий, ориентированный на устройства, для централизованной настройки 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.

Возможно, вы также захотите рассмотреть управление безопасностью, ориентированное на пользователей как альтернативу или дополнительную возможность для подхода, ориентированного на устройства.

Процесс

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 Cloud Console создает политику по умолчанию для Kaspersky Endpoint Security для Windows. Если вы завершили процесс настройки с помощью этого мастера, вам не нужно создавать политику для этого приложения. Перейдите к настройке политики Kaspersky Endpoint Security вручную.

   Если у вас иерархическая структура нескольких групп администрирования, дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами, 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, расположенным в определенном подразделении или группе безопасности Active Directory, имеющим определенную конфигурацию программного обеспечения или имеющим заданные теги. Используйте теги для фильтрации устройств, соответствующих определенным критериям. Например, вы можете создать тег *Windows*, назначить его всем устройствам под управлением операционной системы Windows, а затем указать этот тег в правилах активации профиля политики. В результате на устройствах под управлением операционной системы Windows установленные 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**

   Kaspersky Security Center Cloud Console автоматически синхронизирует Сервер администрирования с управляемыми устройствами несколько раз в час. 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 Cloud Console 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.

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 Cloud Console создает политику по умолчанию для Kaspersky Endpoint Security. Если вы завершили процесс настройки с помощью этого мастера, вам не нужно создавать политику для этого приложения. Перейдите к настройке политики Kaspersky Endpoint Security вручную.

   Если у вас иерархическая структура нескольких групп администрирования, дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами, 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**

   Kaspersky Security Center Cloud Console автоматически синхронизирует Сервер администрирования с управляемыми устройствами несколько раз в час. 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 Cloud Console 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.

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.

См. таблицу сравнения, в которой подробно описано как применяются параметры, приведенные ниже, в зависимости от используемой операционной системы.

Вкладка Общие

На этой вкладке можно изменить состояние политики и настроить наследование параметров политики:

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:
  - **Активна**
  - **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.

Вкладка Настройка событий

На этой вкладке можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности в следующих разделах на вкладке **Настройка событий**:

- **Отказ функционирования**
- **Предупреждение**
- **Информационное сообщение**

В каждом разделе в списке типов событий отображаются названия событий и время хранения событий на Сервере администрирования по умолчанию (в днях). По кнопке **Свойства** можно настроить параметры регистрации и уведомления о событиях, выбранных в списке. По умолчанию общие настройки уведомлений, указанные для всего Сервера администрирования, используются для всех типов событий. Однако можно изменить определенные параметры для заданных типов событий.

Вкладка Параметры приложения

Параметры

В разделе **Параметры** можно настроить параметры политики Агента администрирования:

- **Распространять файлы только через точки распространения**

  Если этот параметр включен, клиентские устройства получают обновления только через точки распространения, а не напрямую с серверов обновлений.

  Если этот параметр выключен, клиентские устройства могут получать обновления из разных источников: напрямую с серверов обновлений, из локальной или сетевой папки.

  По умолчанию параметр выключен.

- **Максимальный размер очереди событий (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 Windows). 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.

  Обратите внимание, что утилита klmover используется только для перемещения управляемых устройств под управление виртуального Сервера администрирования.

  По умолчанию параметр выключен.

Хранилища

В разделе **Хранилища** можно выбрать типы объектов, информацию о которых Агент администрирования будет отправлять на Сервер администрирования. Если в политике Агента администрирования наложен запрет на изменение параметров, указанных в этом разделе, эти параметры недоступны для изменения:

- **Информация об установленных приложениях**
- **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 обновлениях Центра обновления Windows, которые необходимо установить на клиентских устройствах.

  Иногда, даже если параметр выключен, обновления отображаются в свойствах устройства в разделе **Применимые обновления**. Это может произойти, если, например, устройства организации имеют уязвимости, которые могут быть закрыты с помощью этих обновлений.

  По умолчанию параметр включен. Доступен только для Windows.

  Информация 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**

Обновления и уязвимости в приложениях

В разделе **Обновления и уязвимости в приложениях** можно настроить поиск обновлений Windows, а также включить проверку исполняемых файлов на наличие уязвимостей. Параметры раздела **Обновления и уязвимости в приложениях** доступны только для устройств под управлением Windows:

- В блоке параметров **Режим поиска Центра обновления Windows** можно выбрать режим поиска обновлений:

  - **Активный**

    Если выбран этот вариант, Сервер администрирования с помощью Агента администрирования инициирует обращение агента обновлений Windows на клиентском устройстве к источнику обновлений: Windows Update Servers или WSUS. Далее Агент администрирования передает на Сервер администрирования информацию, полученную от Агента Центра обновления Windows.

    Этот параметр применяется, только если включен параметр **Соединяться с сервером обновлений для актуализации данных** задачи *Поиск уязвимостей и требуемых обновлений*.

    По умолчанию выбран этот вариант.

  - **Пассивный**

    Если выбран этот вариант, Агент администрирования периодически передает на Сервер администрирования информацию об обновлениях, полученную при последней синхронизации агента обновлений Windows с источником обновления. Если синхронизация агента обновлений Windows с источником обновления не выполняется, данные об обновлениях на Сервере администрирования устаревают.

    Выберите этот параметр, если вы хотите получать обновления из кеша источника обновлений.

  - **Выключен**

    Если выбран этот вариант, Сервер администрирования не запрашивает информацию об обновлениях.

    Выберите этот параметр, если, например, вы хотите сначала протестировать обновления на локальном устройстве.

- **Проверять исполняемые файлы на наличие уязвимостей при запуске**

  Если параметр включен, при запуске исполняемых файлов выполняется их проверка на наличие уязвимостей.

  По умолчанию параметр выключен.

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.

Совместный доступ к рабочему столу Windows

В разделе **Совместный доступ к рабочему столу Windows** можно включить и настроить аудит действий администратора на удаленном устройстве пользователя при использовании общего доступа к рабочему столу. Параметры раздела **Совместный доступ к рабочему столу Windows** доступны только для устройств под управлением Windows:

- **Включить аудит**

  Если параметр включен, аудит действий администратора на удаленном устройстве включен. Записи о действиях администратора на удаленном устройстве сохраняются:

  - в журнале событий на удаленном устройстве;
  - в файле с расширением syslog, который находится в папке установки Агента администрирования на удаленном устройстве;
  - в базе событий Kaspersky Security Center Cloud Console.

  Аудит действий администратора доступен при выполнении следующих условий:

  - лицензия на Системное администрирование уже используется;
  - у администратора есть право на запуск общего доступа к рабочему столу удаленного устройства.

  Если параметр выключен, аудит действий администратора на удаленном устройстве выключен.

  По умолчанию параметр выключен.

- **Маски файлов, чтение которых нужно отслеживать**

  В списке содержатся маски файлов. Когда аудит включен, приложение отслеживает чтение администратором файлов, соответствующих маскам, и сохраняет информацию о чтении файлов. Список доступен, когда установлен флажок **Включить аудит**. Можно изменять маски файлов и добавлять в список новые маски. Новые маски файлов нужно указывать в списке с новой строки.

  По умолчанию указаны маски файлов *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Маски файлов, изменение которых нужно отслеживать**

  В списке содержатся маски файлов на удаленном устройстве. Когда аудит включен, приложение отслеживает изменение администратором файлов, соответствующих маскам, и сохраняет информацию об изменении файлов. Список доступен, когда установлен флажок **Включить аудит**. Можно изменять маски файлов и добавлять в список новые маски. Новые маски файлов нужно указывать в списке с новой строки.

  По умолчанию указаны маски файлов *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Управление патчами и обновлениями

В разделе **Управление патчами и обновлениями** можно настроить получение и распространение обновлений и установку патчей на управляемые устройства: включить или выключить параметр **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**.

Подключения

Раздел **Подключения** включает три вложенных раздела:

- **Сеть**
- **Профили соединений**
- **Расписание соединений**

В разделе **Сеть** можно настроить параметры подключения к Серверу администрирования, включить возможность использования UDP-порта и указать его номер.

- В блоке **Подключение к Серверу администрирования** можно указать следующие параметры:
  - **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 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.

  Если клиентское устройство работает под управлением операционной системы Windows XP Service Pack 2, встроенный сетевой экран блокирует UDP-порт с номером 15000. Этот порт требуется открыть вручную.

- **Использовать точку распространения для принудительного подключения к Серверу**

  Выберите этот параметр, если в окне параметров точки распространения вы выбрали **Включено**. Иначе точка распространения не будет выполнять роль push-сервера.

В подраздел **Профили соединений** новые элементы не могут быть добавлены в список **Профили подключения к Серверу администрирования**, так как кнопка **Добавить** неактивна. Предустановленные профили соединений тоже невозможно изменить.

В разделе **Расписание соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования:

- **Подключаться при необходимости**

- **Подключаться в указанные периоды**

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. Параметры опроса сети доступны только для устройств под управлением Windows. Вы можете использовать следующие параметры, чтобы включить опрос и настроить его расписание:

- **Сеть Windows**

  Если параметр включен, точка распространения 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 не выполняет опрос сети.

  По умолчанию параметр выключен.

- **IP-диапазоны**

  Если параметр включен, точка распространения автоматически опрашивает IP-диапазоны в соответствии с расписанием, настроенным по ссылке **Настроить расписание опроса**.

  Если параметр выключен, точка распространения не выполняет опрос IP-диапазонов.

  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.

- **Имя пользователя**

- **Пароль**

Прокси-сервер KSN (точки распространения)

В разделе **Прокси-сервер KSN (точки распространения)** вы можете настроить приложение так, чтобы точка распространения использовалась для пересылки 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.

  > Такая возможность не поддерживается для точек распространения под управлением Linux или macOS.

  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 параметр **Я принимаю условия использования Kaspersky Security Network** включен 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.

- **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.

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.

Сравнение параметров политики Агента администрирования по операционным системам

В таблице ниже показано, какие параметры политики Агента администрирования можно использовать для настройки Агента администрирования для конкретной операционной системы.

Параметры политики Агента администрирования: сравнение по операционным системам

Раздел Политики	Windows	macOS	Linux
Общие	✓	✓	✓
Настройка событий	✓	✓	✓
Параметры	✓	✓ Кроме флажка **Использовать пароль деинсталляции**.	✓ Кроме флажка **Использовать пароль деинсталляции**.
Хранилища	✓	✓ Функциональность **Информация о реестре оборудования** доступна.	✓ Доступна функциональность: • **Информация об установленных приложениях** • **Информация о реестре оборудования**
Обновления и уязвимости в приложениях	✓	—	—
Управление перезагрузкой	✓	—	—
Совместный доступ к рабочему столу Windows	✓	—	—
Управление патчами и обновлениями	✓	—	—
Подключения → Сеть	✓	✓ Кроме флажка **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**.	✓ Кроме флажка **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**.
Подключения → Расписание соединений	✓	✓	✓
Опрос сети точками распространения	✓ Доступны следующие параметры: • **Сеть Windows** • **IP-диапазоны** • **Контроллеры доменов** (Microsoft Active Directory)	—	✓ Доступны следующие параметры: • **IP-диапазоны** • **Контроллеры доменов** (Microsoft Active Directory, Samba как Active Directory)
Параметры сети для точек распространения	✓	✓	✓
Прокси-сервер KSN (точки распространения)	✓	—	✓

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**.

Задачи

В этом разделе описаны задачи, которые используются в Kaspersky Security Center Cloud Console.

О задачах

Kaspersky Security Center Cloud Console 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. Задачи могут выполняться на Сервере администрирования и на устройствах.

На устройствах выполняются следующие типы задач:

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

  Локальные задачи может изменять не только администратор средствами администрирования, но и пользователь 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.

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

Для каждого приложения вы можете создавать несколько групповых задач, задач для наборов устройств 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 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), NetBIOS- или DNS-имя.

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

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

- Указать выборку устройств.

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

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

Задачи 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

Вы можете создать задачу в списке задач. Также можно выбрать устройства в списке **Активы (Устройства)** и создать задачу, назначенную выбранным устройствам.

Чтобы создать задачу в списке задач:

1. В главном окне приложения перейдите в раздел **Управление активами → Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте шагам мастера.
3. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
4. Нажмите на кнопку **Готово**.

Задача будет создана и отобразится в списке задач.

Чтобы создать задачу, назначенную выбранным устройствам:

В главном окне приложения перейдите в раздел **Управление активами → Активы (Устройства)**.

Отобразится список управляемых устройств.

1. 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.
2. Нажмите на кнопку **Запустить задачу** и выберите **Создать задачу**.

   Запустится мастер создания задачи.

   На первом шаге мастера вы можете удалить устройства, выбранные для включения в область применения задачи. Следуйте инструкциям мастера.
3. Нажмите на кнопку **Готово**.

Задача создана для выбранных устройств.

Просмотр списка задач

Вы можете просмотреть список задач, созданных в Kaspersky Security Center Cloud Console.

Чтобы просмотреть список задач,

в главном окне приложения перейдите в раздел **Управление активами → Задачи**.

Отобразится список задач. Задачи сгруппированы по названиям приложений, к которыми они относятся. Например, задача *Удаленная деинсталляция приложения* относится к Серверу администрирования, а задача *Поиск уязвимостей и требуемых обновлений* относится к Агенту администрирования.

Чтобы просмотреть свойства задачи,

нажмите на имя задачи.

Окно свойств задачи отображается с несколькими именными вкладками. Например, **Тип задачи** отображается на вкладке **Общие**, а расписание задачи на вкладке **Расписание**.

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 **Активы (Устройства)** и запустить для них существующую задачу.

Чтобы запустить задачу вручную:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Задачи**.
2. В отобразившемся списке задач установите флажок напротив задачи, которую вы хотите запустить.
3. Нажмите на кнопку **Запустить**.

Задача будет запущена. Вы можете проверить статус задачи в 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.

Чтобы запустить задачу для выбранных устройств:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**. Отобразится список управляемых устройств.

   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.

2. Нажмите на кнопку **Запустить задачу** и выберите **Применить существующую задачу**.

   Отобразится список существующих задач.

3. Выбранные устройства отображаются над списком задач. При необходимости вы можете удалить устройство из этого списка. Вы можете удалить все устройства, кроме одного.

4. Выберите необходимую задачу в списке. Вы можете использовать поле поиска над списком для поиска задачи по ее названию. Можно выбрать только одну задачу.

5. Нажмите на кнопку **Сохранить и запустить задачу**.

Выбранная задача сразу запускается для выбранных устройств. Параметры запуска по расписанию в задаче не меняются.

Общие параметры и свойства 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.

- Окно Выбор устройств, 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**

    В этом случае задача назначается набору устройств. Можно указать устройство одним из следующих способов:

    - Укажите IP-адрес, NetBIOS-имя или DNS-имя устройства.
    - Укажите IP-диапазон.

      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.

    - Выберите устройства, обнаруженные Сервером администрирования, включая нераспределенные устройства.

      Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

- **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.

- 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.

- Параметры перезагрузки операционной системы:

  - **Не перезагружать**

    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.

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.

- Параметры расписания задачи:

Типы расписаний могут изменяться в зависимости от задачи.

- **Параметры Запуск задачи:**
  - **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.

  - **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 загрузке обновлений в хранилище**

  Когда новые обновления загружаются в хранилища точек распространения, Kaspersky Security Center Cloud Console запускает все задачи с таким расписанием. Агент администрирования проверяет наличие обновлений во время периодической синхронизации (называемой также пульсом) между управляемым устройством и Сервером администрирования.

  Например, вы можете использовать это расписание для задачи Обновление, связанной с приложением безопасности, таким как Kaspersky Endpoint Security.

  Если Агент администрирования на управляемом устройстве не обнаруживает новых обновлений в течение 25 часов или дольше, то Kaspersky Security Center Cloud Console запускает на этом устройстве все задачи с таким расписанием. Эти задачи выполняются каждый час, пока не будут обнаружены новые обновления. Kaspersky Security Center Cloud Console также выполняет эти задачи каждый час, если между управляемым устройством и точкой распространения, которая загружает обновления в хранилище, нет связи.

- **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**.

Параметры расписания могут **зависеть от местного часового пояса операционной системы устройства**.

Корреляция между локальным часовым поясом операционной системы устройства и временем запуска задачи

Расписание задачи	Используется местное время
Один раз	Нет
Каждые N минут	Нет
Каждый N час	Нет
Каждые N дней	Да
По дням недели	Да
Ежемесячно	Да
Ежемесячно в выбранный день	Да
При загрузке обновлений в хранилище	Другое условие для запуска задачи (соответствует названию расписания)
При обнаружении вирусной атаки	Другое условие для запуска задачи (соответствует названию расписания)
По завершении другой задачи	Другое условие для запуска задачи (соответствует названию расписания)
Немедленно	Другое условие для запуска задачи (соответствует названию расписания)
Вручную	Другое условие для запуска задачи (соответствует названию 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 выключен.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать 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.

- **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.

- Уведомления:

  - Блок **Сохранять информацию о результатах**:

    - **Сохранять все события**
    - **Сохранять события, связанные с ходом выполнения задачи**
    - **Сохранять только результат выполнения задачи**

- **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 журнале событий Windows каждого клиентского устройства.

  По умолчанию параметр выключен.

- **Уведомлять только об ошибках**

- **Уведомлять по электронной почте**

- Параметры области действия задачи

- **Исключения из области**

  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 Cloud Console 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 **Управление активами** → **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 Cloud Console 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 **Управление активами → 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 NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

     Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить 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)**.

Просмотр результатов выполнения задач, хранящихся на Сервере администрирования

Kaspersky Security Center Cloud Console позволяет просматривать результаты выполнения групповых задач, задач для наборов устройств и задач Сервера администрирования.

Чтобы посмотреть результаты выполнения задачи:

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.

Управление клиентскими устройствами

Kaspersky Security Center Cloud Console 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 → Активы (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 Cloud Console.

- **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**

    Windows-домен или рабочая группа, в которую входит устройство.

  - **DNS-имя**

    Имя DNS-домена клиентского устройства.

  - **NetBIOS-имя**

    Имя клиентского устройства в сети Windows.

  - **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.

- 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 Cloud Console.

- **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, редактировать 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 Консоли администрирования или в Kaspersky Security Center Cloud Console).
    - Просмотреть список рекомендуемых исправлений для уязвимости.
    - Вручную указать обновления программного обеспечения для закрытия уязвимости (в Консоли администрирования или в Kaspersky Security Center Cloud 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.

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.
- `Administration 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.
- `Numbers of the Administration Server SSL ports` – номера допустимых портов для подключения к Серверу администрирования при использовании защищенного канала.
- `Numbers of the Administration 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`.
- `Administration Server 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.
  - `available` – 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.

- `Numbers of 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.
- `Synchronization interval (min)` – стандартный интервал синхронизации.
- `Connection timeout (in seconds)` – время ожидания соединения.
- `Send / receive timeout (in seconds)` – время ожидания соединения для операций чтения-записи.
- `Device 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:

- `Total number of synchronization requests` – количество попыток подключения клиентского устройства к Серверу администрирования.
- `The number of successful synchronization request` – количество успешных попыток подключения клиентского устройства к Серверу администрирования.
- `Total number of synchronizations` – количество попыток синхронизации параметров клиентского устройства с параметрами Сервера администрирования.
- `The number of successful synchronizations` – количество успешных попыток синхронизации параметров клиентского устройства с Сервером администрирования.
- `Date/time of the last request for synchronization` – дата и время последнего подключения.

При анализе соединения между Сервером администрирования и Агентом администрирования необходимо использовать параметры `Total number of synchronization requests` и `The number of successful synchronization request`. 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 `Total number of synchronizations` и `The number of successful synchronization request` не изменяются.

Подробнее об устранении проблем с подключением Агента администрирования к Серверу администрирования см. Kaspersky Security Center Cloud Console FAQ.

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 Cloud Console 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 Cloud Console 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.

Вы можете выбрать одно или несколько устройств в выборке устройств и нажать на кнопку **Новая задача**, чтобы создать задачу, которая будет применена к этим устройствам.

Чтобы переместить выбранные устройства из выборки устройств в другую группу администрирования, нажмите на кнопку **Переместить в группу** и выберите целевую группу администрирования.

Создание выборки устройств

Чтобы создать выборку устройств:

1. В главном окне 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 указанный Windows-домен.

- **Группа администрирования**

  Будут отображаться устройства, входящие в указанную группу администрирования.

- **Описание**

  Текст, который содержится в окне свойств устройства: в поле **Описание** раздела **Общие**.

Для описания текста в поле **Описание** допустимо использовать следующие символы:

- Внутри одного слова:
  - *****. Заменяет любую строку длиной 0 и более символов.

    Пример:

    Для описания слов **Сервер**, **Серверный** или Серверная можно использовать строку **Сервер***.

  - **?.** Заменяет любой один символ.

    Пример:

    Для описания слов **Окно** или **Окна** можно использовать строку **Окн?**.

    Звездочка (*****) или вопросительный знак (**?**) не могут использоваться как первый символ в описании текста.

- Для связи нескольких слов:
  - Пробел. Отображает все устройства, описания которых содержат любое из перечисленных слов.

    Пример:

    Для описания фразы, содержащей слово **Подчиненный** или **Виртуальный** можно использовать строку **Подчиненный Виртуальный**.

  - **+**. При написании перед словом обозначает обязательное наличие слова в тексте.

    Пример:

    Для описания фразы, содержащей и слово **Подчиненный**, и слово **Виртуальный**, можно использовать строку **+Подчиненный+Виртуальный**.

  - **-**. При написании перед словом обозначает обязательное отсутствие слова в тексте.

    Пример:

    Для описания фразы, в которой должно присутствовать слово **Подчиненный**, но должно отсутствовать слово **Виртуальный**, можно использовать строку **+Подчиненный-Виртуальный**.

  - **"<фрагмент текста>"**. Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте.

    Пример:

    Для описания фразы, содержащей словосочетание **Подчиненный Сервер**, можно использовать строку **"Подчиненный Сервер"**.

- **IP-диапазон**

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

  По умолчанию параметр выключен.

- **Под управлением другого Сервера администрирования**

  Выберите одно из следующих значений:

  - **Да**. Правило перемещения устройств применяется только к клиентским устройствам, управляемым другими Серверами администрирования. Эти Серверы отличаются от Сервера, на котором вы настраиваете правило перемещения устройств.
  - **Нет**. Правило перемещения устройств применяется только к клиентским устройствам, управляемым текущим Сервером администрирования.
  - **Значение не выбрано**. Условие не применяется.

В разделе **Active Directory** можно настроить критерии включения устройств в выборку на основании их данных Active Directory:

- **Устройство в подразделении Active Directory**

  Если этот параметр включен, в выборку будут включаться устройства из организационной единицы Active Directory, указанного в поле ввода.

  По умолчанию параметр выключен.

- **Включать дочерние подразделения**

  Если этот параметр включен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы Active Directory.

  По умолчанию параметр выключен.

- **Устройство является членом группы Active Directory**

  Если этот параметр включен, в выборку будут включаться устройства из группы Active Directory, указанной в поле ввода.

  По умолчанию параметр выключен.

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.

В разделе **Облачные сегменты** можно настроить критерии включения устройств в выборку в соответствии с облачными сегментами:

- **Устройство находится в облачном сегменте**

  Если этот параметр включен, вы можете выбрать устройства из облачных сегментов AWS, Azure и Google.

  Если также включен параметр **Включать дочерние объекты**, то поиск ведется по всем вложенным объектам указанного сегмента.

  В результаты поиска включаются устройства только из выбранного сегмента.

- **Устройство обнаружено с помощью API**

  В раскрывающемся списке можно выбрать, обнаруживается ли устройство средствами API:

  - **Да**. Устройство обнаруживается с помощью AWS, Azure или Google API.
  - **Нет**. Устройство не обнаруживается с помощью AWS, Azure или Google API. То есть устройство либо находится вне облачного окружения, либо находится в облачном окружении, но по каким-то причинам недоступно для поиска с помощью API.
  - Не задано. Это условие 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**

  Имя устройства в Windows-сети. Устройство с указанным именем будет включено в выборку.

- **Описание**

  Описание устройства или оборудования. Устройства с описанием, указанным в поле, будут включены в состав выборки.

Описание устройства в произвольной форме можно ввести в окне свойств устройства. В поле поддерживается полнотекстовый поиск.

- **Поставщик устройства**

  Название производителя устройства. Устройства, изготовленные производителем, указанным в поле, будут включены в состав выборки.

  Название производителя можно ввести в окне свойств устройства.

- **Серийный номер**

  Оборудование с серийным номером, указанным в поле, будет включено в выборку.

- **Инвентарный номер**

  Оборудование с инвентарным номером, указанным в поле, будет включено в выборку.

- **Пользователь**

  Оборудование пользователя, указанного в поле, будет включено в выборку.

- **Расположение**

  Место расположения устройства или оборудования (например, в офисе или филиале). Компьютеры или другие устройства с расположением, указанным в поле, будут включены в состав выборки.

  Расположение оборудования в произвольной форме можно ввести в окне свойств оборудования.

- **Частота процессора (МГц) от**

  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**

  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.

  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.

- **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 Cloud Console:

  - **Да**. Приложение включает в выборку устройства, которые находятся под управлением Kaspersky Security Center Cloud Console.
  - **Нет**. Приложение включает в выборку устройства, которые не находятся под управлением Kaspersky Security Center Cloud Console.
  - **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**

  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*.

  Если этот параметр включен, поиск клиентских устройств выполняется по количеству найденных вирусов. В полях ввода можно задать нижнее и верхнее значения количества найденных вирусов.

По умолчанию параметр выключен.

Подраздел **Компоненты приложения** содержит список компонентов тех приложений, которые имеют соответствующие плагины управления, установленные в Kaspersky Security Center Cloud 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. Обратите внимание, что список пользователей отфильтрован и отображаются внутренние пользователи. В результаты поиска будут включены устройства, на которых последний вход в систему выполнялся выбранным пользователем.

- **Пользователь, уже выполнявший вход в систему**

  Если этот параметр включен, вы можете выбрать учетную запись пользователя, для которой настроили критерий. Обратите внимание, что список пользователей отфильтрован и отображаются внутренние пользователи. В результаты поиска будут включены устройства, на которых указанный пользователь когда-либо выполнял вход в систему.

Экспорт списка устройств из выборки устройств

Kaspersky Security Center Cloud Console 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**.

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.

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. Выберите имя требуемой группы администрирования.

   Откроется окно свойств группы администрирования.
3. В окне свойств выберите 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.

5. В разделе **Активность устройств** включите или выключите следующие параметры:

- **Уведомлять администратора, если устройство неактивно больше (сут)**

  Если этот параметр включен, администратор получает уведомления о неактивности устройств. В поле ввода можно задать интервал времени, по истечении которого будет сформировано событие **Устройство долго не проявляет активности в сети**. Временной интервал, установленный по умолчанию, составляет 7 дней.

  По умолчанию параметр включен.

- **Удалять устройство из группы, если оно неактивно больше (сут)**

  Если этот параметр включен, вы можете указать временной интервал, после которого устройство автоматически удаляется из группы администрирования. Временной интервал, установленный по умолчанию, составляет 60 дней.

  По умолчанию параметр включен.

6. Нажмите на кнопку **Сохранить**.

Ваши изменения сохранены и применены.

О статусах устройства

Kaspersky Security Center Cloud Console 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 Cloud Console учитывает видимость устройства в сети (см. таблицу ниже). Если Kaspersky Security Center Cloud Console 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 вирусов, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение.	Более 0.
Уровень постоянной защиты отличается от уровня, установленного администратором	Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства.	• Остановлена. • Приостановлена. • Выполняется.
Давно не выполнялся поиск 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.
Требуется перезагрузка	Устройство видимо в сети, но приложение требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин.	Более чем 0 минут.
Установлены несовместимые приложения	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые приложения.	• Переключатель выключен. • Переключатель включен.
Обнаружены уязвимости в приложениях	Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи *Поиск уязвимостей и требуемых обновлений* на устройстве обнаружены уязвимости в приложениях с заданным уровнем критичности.	• Предельный. • Высокий. • Средний. • Игнорировать, если невозможно закрыть уязвимость. • Игнорировать, если обновление назначено к установке.
Срок действия лицензии истек	Устройство видимо в сети, но срок действия лицензии истек.	• Переключатель выключен. • Переключатель включен.
Срок действия лицензии скоро истекает	Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.	Менее 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.	• 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 *Приостановлено*.	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 Cloud Console 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*.

Когда Kaspersky Security Center Cloud Console присваивает устройству статус, для некоторых условий (см. столбец "Описание условий") учитывается видимость устройств в сети. Например, если управляемому устройству был присвоен статус *Критический*, так как выполнено условие Базы устарели, а затем для устройства стало видимо в сети, то устройству присваивается статус *OK*.

Настройка переключения статусов устройств

Вы можете изменить условия присвоения статусов *Критический* или *Предупреждение* устройству.

Чтобы изменить статус устройства на Критический:

1. В главном окне 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 **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 **ОК**.

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**.

При выполнении заданных условий управляемому устройству присваивается статус *Предупреждение*.

Смена Сервера администрирования для клиентских устройств

Вы можете сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером с помощью задачи **Смена Сервера администрирования**. После завершения задачи выбранные клиентские устройства будут под управлением указанного Сервера администрирования. Вы можете переключать управление устройством между следующими Серверами администрирования:

- главным Сервер администрирования и одним из его виртуальных Серверов администрирования;
- двумя виртуальными Серверами администрирования одного и того же главного Сервера администрирования.

Чтобы сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером:

1. В главном окне приложения перейдите в раздел **Управление активами → Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. На шаге **Параметры новой задачи** укажите следующие параметры:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Security Center Cloud Console**.

   b. В поле **Тип задачи** выберите **Смена Сервера администрирования**.

   c. В поле **Название задачи** укажите название создаваемой задачи.

   Имя 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 NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

  Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить 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 **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

5. На следующем шаге подтвердите свое согласие с условиями смены Сервера администрирования для клиентских устройств.

6. На следующем шаге выберите виртуальный Сервер администрирования, который вы хотите использовать для управления выбранными устройствами.

7. На шаге **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 вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи.

   Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

9. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.

10. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

11. В окне свойств задачи укажите общие параметры задачи в соответствии с вашими требованиями.

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.

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 Cloud Console перейдите в раздел **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.
2. Выберите нужное устройство и нажмите на кнопку **Удалить атрибут "Управляется другим Сервером администрирования"**.

Атрибут **Под управлением другого Сервера администрирования** будет сброшен.

Создание профилей подключения к Серверу администрирования

Чтобы автономные пользователи могли изменять способ подключения Агента администрирования к Серверу администрирования, необходимо настроить профили подключения к Серверу администрирования.

Чтобы создать профиль соединения:

1. В главном окне приложения перейдите в раздел **Управление активами** и выполните одно из следующих действий:

   - Если вы хотите создать профиль соединения для группы управляемых устройств, перейдите в раздел **Политики** и нажмите на **Агент администрирования Kaspersky Security Center**.

   - Если вы хотите создать профиль соединения для определенного управляемого устройства, перейдите в раздел **Активы (Устройства)** и нажмите на имя устройства. В открывшемся окне перейдите на вкладку **Приложения** и нажмите на кнопку **Агент администрирования Kaspersky Security Center**.

   Откроется окно свойств политики Агента администрирования.

2. Перейдите на вкладку **Параметры приложения**, а затем перейдите в раздел **Подключения**.

3. В разделе **Профили соединений** нажмите на кнопку **Параметры**.

   В разделе **Профили подключения к Серверу администрирования** отображается таблица профилей соединения.

   > Вы не можете просматривать, изменять или удалять профили соединения **Домашний Сервер администрирования** и **Офлайн-режим**.

4. Нажмите на кнопку **Добавить** и открывшемся окне укажите имя профиля.

   > Имя должно быть уникальным. Вы не можете использовать одно и то же имя для нескольких профилей.

5. При необходимости установите флажки в следующих полях:

   - **Включить автономный режим, когда Сервер администрирования недоступен**.

   - **Использовать прокси-сервер**.

Если вы выбрали этот параметр:

- Укажите информацию в полях **Адрес** и **Номер порта**.
- При необходимости установите флажок **Аутентификация на прокси-сервере** и укажите имя пользователя и пароль в соответствующих полях.

6. Нажмите на кнопку **Сохранить**.

Новый профиль отобразится в таблице профилей соединения. Вы можете использовать его при настройке параметров **Сетевого месторасположения**.

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.

Вы можете изменять и удалять профили соединения.

Чтобы изменить профиль соединения:

1. В таблице профилей подключения нажмите на имя профиля соединения, который вы хотите изменить.
2. Внесите все необходимые изменения и нажмите на кнопку **Сохранить**.

Изменения применены к профилю соединения.

Чтобы удалить профиль соединения:

1. В таблице профилей соединения установите флажки рядом с профилями соединения, которые вы хотите удалить.
2. Нажмите на кнопку **Удалить**.

Выбранные профили соединения будут удалены.

О кластерах и массивах серверов

Kaspersky Security Center Cloud Console 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 **Активы (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 Cloud Console 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** → **Активы (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 Cloud Console 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.

Теги устройств

Kaspersky Security Center Cloud Console позволяет назначать теги устройствам. *Тег* представляет собой идентификатор устройства, который можно использовать для группировки, описания, поиска устройств. Назначенные устройствам теги можно использовать при создании выборок устройств, при поиске устройств и при распределении устройств по группам администрирования.

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

Автоматическое назначение тегов устройствам происходит при выполнении определенных правил. Каждому тегу соответствует отдельное правило. Правила могут применяться к сетевым свойствам устройства, операционной системе, установленным на устройстве приложениям и другим свойствам устройства. Например, если в вашей сети есть устройства под управлением Windows, Linux и macOS, вы можете настроить правило, которое будет назначать тег `[Linux]` всем устройствам с операционной системой Linux. Затем можно использовать этот тег при создании выборки устройств, чтобы отобрать все устройства с операционной системой Linux 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 **Управление активами** → **Теги** → **Теги устройств**.
2. Нажмите на кнопку **Добавить**.

   Отобразится окно создания тега.
3. В поле **Тег** введите название тега.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Новый созданный тег появляется в списке тегов устройства.

Изменение тегов устройств

Чтобы переименовать тег устройства:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Теги** → **Теги устройств**.
2. Выделите тег, который требуется переименовать.

   Откроется окно свойств тега.
3. В поле **Тег** измените название тега.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Обновленный тег появится в списке тегов устройства.

Удаление тегов устройств

Чтобы удалить тег устройства:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Теги** → **Теги устройств**.
2. В списке выберите теги устройства, которые вы хотите удалить.

3. Нажмите на кнопку **Удалить**.

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

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

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

Удаленный тег не удаляется автоматически с устройства, если этот тег назначен устройству приложением или Агентом администрирования. Для того чтобы 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 **Управление активами → Теги → Теги устройств**.

2. Перейдите по ссылке **Просмотреть устройства** рядом с названием тега, для которого вы хотите посмотреть список назначенных устройств.

   Вы будете перенаправлены в раздел **Активы (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 → Активы (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 устройствам вручную

Чтобы 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 добавить новый тег, выберите пункт **Создать тег** и укажите имя тега.
   - Чтобы выбрать существующий тег, выберите пункт **Назначить существующий тег** и в раскрывающемся списке выберите нужный тег.
4. Нажмите на кнопку **ОК**, чтобы применить изменения.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Выбранный тег будет назначен устройству.

Чтобы назначить тег нескольким устройствам:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.
2. Выберите устройства, которым вы хотите назначить тег.
3. Нажмите на **Теги** и выберите пункт **Назначить** из раскрывающегося списка.
4. В открывшемся окне выберите тег из раскрывающегося списка.

   При необходимости можно выбрать несколько тегов.

   Также можно выполнить следующее:

   - Изменить тег, нажав на значок **Изменить** ().

     Укажите новое имя тега и нажмите на кнопку **Сохранить**.

     Обратите внимание, что тег также будет переименован в списке тегов устройства.

   - Удалить тег, нажав на значок **Удалить** ().

В появившемся окне нажмите на кнопку **Удалить**.

Обратите внимание, что тег также будет удален с Сервера администрирования.

5. Нажмите на кнопку **Сохранить**.

Теги назначены выбранным устройствам. Вы можете удалить назначенные теги.

Снятие назначенных тегов с устройств

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.

Чтобы снять назначенный тег с устройства:

1. В главном окне приложения перейдите в раздел **Управление активами → Активы (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 **Да**.

Тег будет снят с устройства.

Чтобы удалить теги с нескольких устройств:

1. В главном окне приложения перейдите в раздел **Управление активами → Активы (Устройства)**.
2. Выберите устройства, теги которых вы хотите удалить.
3. Нажмите на **Теги** и в раскрывающемся списке выберите пункт **Отменить назначение**.
4. В открывшемся окне установите флажки рядом с тегами, которые вы хотите удалить.

В окне отображаются все теги, назначенные всем устройствам, которые вы выбрали на шаге 2.

5. Нажмите на кнопку **Сохранить**.

Теги будут сняты с устройств.

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 **Управление активами** → **Теги** → **Правила автоматического назначения тегов**.
- В главном окне приложения перейдите в раздел **Управление активами** → **Теги** → **Теги устройств**, а затем перейдите по ссылке **Настроить 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 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**.

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

      Название может содержать не более 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 может содержать не более 256 символов. Название условия должно быть уникальным в рамках одного правила.

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

   - **Сеть** – сетевые свойства устройства (например, имя устройства в сети Windows, принадлежность устройства к домену или к IP-подсети).

     Если для базы данных, которую вы используете для Kaspersky Security Center Cloud Console, 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.

- **Active Directory** – нахождение устройства в подразделении Active Directory и членство устройства в группе Active Directory.
- **Реестр приложений** – наличие на устройстве приложений различных производителей.

7. Нажмите на кнопку **OK**, чтобы сохранить изменения.

   При необходимости можно задать несколько условий для одного правила. В этом случае тег будет назначен устройствам, если для них выполняется хотя бы одно из условий.

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

Созданное правило выполняется на устройствах, управляемых выбранным Сервером администрирования. Если параметры устройства соответствуют условиям правила, этому устройству назначается тег.

В дальнейшем правило применяется в следующих случаях:

- Автоматически, регулярно, в зависимости от загрузки сервера.
- После изменения правила.
- После выполнения правила вручную.
- После того как Сервер администрирования обнаружит изменения, которые соответствуют условиям правила, в параметрах устройства или в параметрах группы, которая содержит это устройство.

Вы можете создать несколько правил назначения тегов. Одному устройству может быть назначено несколько тегов, в случае если вы создали несколько правил назначения тегов и условия этих правил выполняются одновременно. Вы можете просмотреть список всех назначенных тегов в свойствах устройства.

Выполнение правил автоматического назначения тегов устройствам

Когда выполняется правило, тег, указанный в свойствах этого правила, назначается устройству, которое соответствует условиям, указанным в свойствах правила. Можно выполнять только активные правила.

Чтобы выполнить правила автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам.
2. Установите флажки напротив активных правил, которые требуется выполнить.
3. Нажмите на кнопку **Выполнить правило**.

   Выбранные правила будут выполнены.

Удаление правил автоматического назначения тегов с устройств

Чтобы удалить правило автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам.
2. Установите флажок напротив правила, которое требуется удалить.

3. Нажмите на кнопку **Удалить**.

4. В появившемся окне нажмите на кнопку **Удалить** еще раз.

Выбранное правило будет удалено. Тег, указанный в свойствах этого правила, будет снят со всех устройств, которым он был назначен.

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

Управление тегами устройств с помощью утилиты klscflag

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

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

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

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

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

2. Введите одну из следующих команд:

   - Чтобы назначить набор тегов:

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

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

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

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

   - Чтобы назначить новый тег существующему набору тегов:

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

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

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

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

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

3. Перезапустите службу Агента администрирования.

   Утилита klscflag назначит вашему устройству указанные теги.

4. Если вы хотите убедиться, что утилита klscflag успешно назначила указанные теги, просмотрите теги, которые были назначены устройству.

Также можно назначать теги устройств вручную.

Карантин и Файлы резервного хранилища

Приложения защиты "Лаборатории Касперского", установленные на клиентских устройствах, в процессе проверки устройств могут помещать файлы в раздел Карантин или в раздел Файлы резервного хранилища.

Карантин – это специальное хранилище, в которое помещаются файлы, возможно зараженные вирусами или неизлечимые на момент обнаружения.

Файлы резервного хранилища предназначены для хранения резервных копий файлов, которые были удалены или изменены в процессе лечения.

Kaspersky Security Center Cloud Console формирует общий список файлов, помещенных в раздел Карантин или в раздел Файлы резервного хранилища приложениями "Лаборатории Касперского" на устройствах. Агенты администрирования клиентских устройств передают информацию о файлах в разделе Карантин или в разделе Файлы резервного хранилища на Сервер администрирования.

Kaspersky Security Center Cloud Console не копирует файлы из хранилищ на Сервер администрирования. Все файлы размещаются в хранилищах на устройствах.

Загрузка файла из хранилища

Kaspersky Security Center Cloud Console позволяет загружать копии файлов, помещенных приложением безопасности в раздел Карантин или в раздел Файлы резервных копий на клиентском устройстве. Файлы копируются в указанную вами папку.

Вы можете загружать файлы только если выполняется одно из следующих условий: параметр **Не разрывать соединение с Сервером администрирования** включен в параметрах устройства, используется push-сервер или используется шлюз соединения. Иначе загрузка невозможна.

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

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 Файлы резервных копий, 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.

Удаление файлов из хранилища

Чтобы удалить файл, помещенный в раздел Карантин или в раздел Файлы резервных копий:

1. В главном окне приложения перейдите в раздел **Операции** → **Хранилища** и выберите один из следующих разделов:

   - **Карантин**, если вы хотите удалить файл из карантина.

   - **Файлы резервных копий**, если вы хотите удалить файл из резервного хранилища.

2. В зависимости от выбранного хранилища выполните одно из следующих действий:

   - В разделе **Файлы резервных копий** выберите файл из списка и нажмите на кнопку **Удалить**.

   - В разделе **Карантин** удалите файл одним из следующих способов:

     - Установите флажок рядом с именем файла, который нужно удалить, а затем в панели инструментов нажмите на кнопку **Удалить**.

     - Нажмите на имя файла, который нужно удалить, и в открывшемся окне свойств в панели инструментов нажмите на кнопку **Удалить**.

       В этом случае файл будет удален, на экране отобразится соответствующее уведомление, окно со свойствами закроется.

   Приложение безопасности на клиентском устройстве, которое поместило файлы в хранилище (Карантин или Файлы резервных копий), удаляет файлы из этого хранилища.

Удаленная диагностика клиентских устройств

Вы можете использовать удаленную диагностику для удаленного выполнения следующих операций на клиентских устройствах на базе Windows и на базе Linux:

- включения и выключения трассировки, изменения уровня трассировки и загрузки файла трассировки;
- загрузки системной информации и параметров приложения;
- загрузки журналов событий;
- создание файла дампа для приложения;
- запуска диагностики и загрузки результатов диагностики;
- запуск, остановка и перезапуск приложений.

Вы можете использовать журнал событий и диагностические отчеты, загруженные с клиентского устройства, для устранения неполадок самостоятельно. Также если вы обращаетесь в Службу технической поддержки "Лаборатории Касперского", эксперт 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 → Активы (Устройства)**.
   - Если устройство принадлежит к группе нераспределенных устройств, в главном меню перейдите в раздел **Обнаружение устройств и развертывание → Нераспределенные устройства**.
2. Нажмите на имя требуемого устройства.
3. В открывшемся окне свойств устройства выберите вкладку **Дополнительно**.
4. 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 дереве объектов устройства 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 эксперт 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 Kaspersky Security Agent регулируется параметрами Агента администрирования. Поэтому параметры **Включить трассировку** и **Изменить уровень трассировки** выключены для этого компонента на клиентских устройствах под управлением Linux.

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 эксперты 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 эксперта 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

Вы можете загрузить файлы трассировки с клиентского устройства. только если выполняется одно из следующих условий: параметр **Не разрывать соединение с Сервером администрирования** включен в параметрах устройства, используется push-сервер или используется шлюз соединения. Иначе загрузка невозможна.

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

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 трассировки устройства**, где отображается список файлов трассировки.

5. В списке файлов трассировки выберите файл, который вы хотите загрузить.

6. Выполните одно из следующих действий:

   - Загрузите выбранный файл, нажав на кнопку **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.

   Откроется окно **Журналы трассировки устройства**, где отображается список файлов трассировки.

4. В списке файлов трассировки выберите один или несколько файлов, которые вы хотите удалить.

5. Нажмите на кнопку **Удалить**.

Выбранные файлы трассировки удалены.

Загрузка параметров приложений

Вы можете загрузить параметры приложений с клиентского устройства только если выполняется одно из следующих условий: параметр **Не разрывать соединение с Сервером администрирования** включен в параметрах устройства, используется push-сервер или используется шлюз соединения. Иначе загрузка невозможна.

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

Чтобы загрузить с клиентского устройства параметры программ:

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

Вы можете загрузить системную информацию с клиентского устройства на свое устройство только если выполняется одно из следующих условий: параметр **Не разрывать соединение с Сервером администрирования** включен в параметрах устройства, используется push-сервер или используется шлюз соединения. Иначе загрузка невозможна.

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

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.

> 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

Вы можете загружать журналы событий с клиентского устройства на свое устройство только если выполняется одно из следующих условий: параметр **Не разрывать соединение с Сервером администрирования** включен в параметрах устройства, используется push-сервер или используется шлюз соединения. Иначе загрузка невозможна.

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

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.

     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 приложения и загрузка результатов

Чтобы запустить диагностику приложения 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 списке приложений выберите приложение, для которого вы хотите запустить удаленную диагностику.

   Откроется список параметров удаленной диагностики.
4. В разделе **Отчет диагностики** нажмите на кнопку **Выполнить диагностику**.

   Запускается процесс удаленной диагностики и генерируется отчет о диагностике. После завершения 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, который вы хотите запустить на клиентском устройстве. 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.

Создание файла дампа для приложения

Файл дампа приложения позволяет просматривать параметры приложения, работающего на клиентском устройстве, в определенный момент времени. Этот файл также содержит информацию о модулях, которые были загружены для приложения.

> Создание файлов дампа доступно только для 32-разрядных процессов, работающих на клиентских устройствах под управлением Windows. Для клиентских устройств под управлением Linux и для 64-битных процессов эта функция не поддерживается.

Чтобы создать файл дампа для приложения:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Запуск удаленного приложения**.

3. В разделе **Формирование файла дампа процесса** укажите исполняемый файл приложения, для которого вы хотите создать файл дампа.

4. Нажмите на кнопку **Скачать**, чтобы сохранить файл дампа указанного приложения.

   Если указанное приложение не запущено на клиентском устройстве, отобразится сообщение об ошибке.

Удаленное подключение к рабочему столу клиентского устройства

Вы можете получить удаленный доступ к рабочему столу клиентского устройства с помощью Агента администрирования, установленного на устройстве. Удаленное подключение к клиентскому устройству с помощью Агента администрирования возможно и в том случае, если TCP- и UDP-порты клиентского устройства закрыты для доступа.

После подключения к устройству вы получаете полный доступ к информации на этом устройстве и может управлять приложениями, установленными на нем.

Удаленное подключение должно быть разрешено в параметрах операционной системы целевого управляемого устройства. Например, в Windows 10 этот параметр называется **Разрешить подключения удаленного помощника к этому компьютеру** (его можно найти **Панель управления** → **Система и безопасность** → **Система** → **Настройка удаленного доступа**). Если у вас есть лицензия на Системное администрирование, вы можете принудительно включить этот параметр, когда установлено соединение с управляемым устройством. Если у вас нет лицензии, включите этот параметр локально на целевом управляемом устройстве. Если этот параметр выключен, удаленное подключение невозможно.

Чтобы установить удаленное соединение с устройством, у вас должно быть две утилиты:

- Утилита klsctunnel "Лаборатории Касперского". Эта утилита должна храниться на вашей рабочей станции. Вы используете эту утилиту для туннелирования соединения между клиентским устройством и Сервером администрирования.

  Kaspersky Security Center Cloud Console позволяет туннелировать TCP-соединения от Консоли администрирования через Сервер администрирования и далее через Агент администрирования к заданному порту на управляемом устройстве. Туннелирование используется для подключения клиентского приложения, находящегося на устройстве с установленной Консолью администрирования, к TCP-порту на управляемом устройстве, если прямое соединение устройства с Консолью администрирования с устройством невозможно.

  Туннелирование соединения удаленного клиентского устройства с Сервером администрирования необходимо, если на устройстве недоступен порт для соединения с Сервером администрирования. Порт на устройстве может быть недоступен в следующих случаях:

  - Удаленное устройство подключено к локальной сети, в которой используется механизм NAT.
  - Удаленное устройство входит в локальную сеть Сервера администрирования, но его порт закрыт сетевым экраном.

- Стандартный компонент Microsoft Windows "Подключение к удаленному рабочему столу". Подключение к удаленному рабочему столу выполняется с помощью штатной утилиты Windows mstsc.exe в соответствии с параметрами работы этой утилиты.

  Подключение к существующему сеансу удаленного рабочего стола пользователя осуществляется без уведомления пользователя. Как только вы подключаетесь к сеансу, пользователь устройства автоматически отключается от сеанса; пользователь не получает предварительного уведомления.

Для подключения к рабочему столу клиентского устройства должно выполняться одно из следующий условий:

- Клиентское устройство является членом группы администрирования, которая имеет точку распространения с включенным параметром **Не разрывать соединение с Сервером администрирования**.
- В параметрах клиентского устройства включен параметр **Не разрывать соединение с Сервером администрирования**.

  Общее количество клиентских устройств с выбранным параметром **Не разрывать соединение с Сервером администрирования** не может превышать 300.

Чтобы удалено подключиться к рабочему столу клиентского устройства:

1. В главном окне приложения перейдите в раздел **Управление активами → Активы (Устройства)**.
2. Установите флажок напротив устройства, к которому вы хотите получить доступ.
3. Нажмите на кнопку **Подключиться к удаленному рабочему столу**.

   Откроется окно Подключиться к удаленному рабочему столу.
4. Нажмите на кнопку **Скачать**, чтобы загрузить утилиту klsctunnel.
5. Нажмите на кнопку **Копировать в буфер обмена**, чтобы скопировать текст из текстового поля. Этот текст представляет собой двоичный объект данных (BLOB), который содержит параметры, необходимые для установления соединения между Сервером администрирования и управляемым устройством.

   Объект BLOB действителен в течение 3 минут. Если срок его действия истек, снова откройте окно Подключиться к удаленному рабочему столу, чтобы сгенерировать новый объект BLOB.
6. Запустите утилиту klsctunnel.

   Откроется окно утилиты.
7. Вставьте скопированный текст в текстовое поле.
8. Если вы используете прокси-сервер, установите флажок **Использовать прокси-сервер**, а затем укажите параметры подключения к прокси-серверу.
9. Нажмите на кнопку **Открыть порт**.

   Откроется окно входа в систему подключения к удаленному рабочему столу.
10. Укажите учетные данные учетной записи, под которой вы в настоящий момент входите Kaspersky Security Center Cloud Console.
11. Нажмите на кнопку **Подключиться**.

После подключения к клиентскому устройству рабочий стол клиентского устройства доступен в окне удаленного подключения Microsoft Windows.

Подключение к устройствам с помощью совместного доступа к рабочему столу Windows

Вы можете получить удаленный доступ к рабочему столу клиентского устройства с помощью Агента администрирования, установленного на устройстве. Удаленное подключение к клиентскому устройству с помощью Агента администрирования возможно и в том случае, если TCP- и UDP-порты клиентского устройства закрыты для доступа.

Вы можете подключиться к существующему сеансу на клиентском устройстве, не отключая пользователя, работающего в этом сеансе. В этом случае у вас и у пользователя сеанса на устройстве есть совместный доступ к рабочему столу.

Чтобы установить удаленное соединение с устройством, у вас должно быть две утилиты:

- Утилита klsctunnel "Лаборатории Касперского". Эта утилита должна храниться на вашей рабочей станции. Вы используете эту утилиту для туннелирования соединения между клиентским устройством и Сервером администрирования.

  Kaspersky Security Center Cloud Console позволяет туннелировать TCP-соединения от Консоли администрирования через Сервер администрирования и далее через Агент администрирования к заданному порту на управляемом устройстве. Туннелирование используется для подключения клиентского приложения, находящегося на устройстве с установленной Консолью администрирования, к TCP-порту на управляемом устройстве, если прямое соединение устройства с Консолью администрирования с устройством невозможно.

  Туннелирование соединения удаленного клиентского устройства с Сервером администрирования необходимо, если на устройстве недоступен порт для соединения с Сервером администрирования. Порт на устройстве может быть недоступен в следующих случаях:

  - Удаленное устройство подключено к локальной сети, в которой используется механизм NAT.
  - Удаленное устройство входит в локальную сеть Сервера администрирования, но его порт закрыт сетевым экраном.

- Совместный доступ к рабочему столу Windows. При подключении к существующему сеансу удаленного рабочего стола пользователь этого сеанса на устройстве получит от вас запрос на подключение. Информация о процессе удаленной работы с устройством и результатах этой работы не сохраняется в отчетах Kaspersky Security Center Cloud Console.

  Вы можете настроить аудит действий на удаленном клиентском устройстве. В ходе аудита приложение сохраняет информацию о файлах на клиентском устройстве, которые открывал и/или изменял администратор.

Для подключения к рабочему столу клиентского устройства с помощью совместного доступа к рабочему столу Windows требуется выполнение следующих условий:

- На вашей рабочей станции установлена операционная система Microsoft Windows Vista или более поздняя версия.

  Чтобы проверить, включена ли функция совместного доступа к рабочему столу Windows в вашей версии Windows, убедитесь, что ключ CLSID {32BE5ED2-5C86-480F-A914-0FF8885A1B3F} включен в 32-разрядный реестр.

- На клиентском устройстве установлена операционная система Microsoft Windows Vista или более поздняя версия.

- Kaspersky Security Center Cloud Console использует лицензию на управление уязвимостями и исправлениями.
- Клиентское устройство является членом группы администрирования, которая имеет точку распространения с включенным параметром **Не разрывать соединение с Сервером администрирования**, или этот параметр включен в свойствах клиентского устройства.

  Обратите внимание, что общее количество клиентских устройств с включенным параметром **Не разрывать соединение с Сервером администрирования** не может превышать 300.

Чтобы подключиться к рабочему столу клиентского устройства с помощью совместного доступа к рабочему столу Windows:

1. В главном окне приложения перейдите в раздел **Управление активами → Активы (Устройства)**.
2. Установите флажок напротив устройства, к которому вы хотите получить доступ.
3. Нажмите на кнопку **Совместный доступ к рабочему столу Windows**.

   Открывается мастер Совместный доступ к рабочему столу Windows.
4. Нажмите на кнопку **Скачать**, чтобы загрузить утилиту klsctunnel, и дождитесь завершения процесса загрузки.

   Если у вас уже есть утилита klsctunnel, пропустите этот шаг.
5. Нажмите на кнопку **Далее**.
6. Выберите сеанс на устройстве, к которому вы хотите подключиться, а затем нажмите на кнопку **Далее**.
7. На целевом устройстве в открывшемся окне пользователь должен разрешить сеанс совместного доступа к рабочему столу. Иначе сеанс невозможен.

   После того как пользователь подтвердит сеанс совместного доступа к рабочему столу, мастер откроет следующий шаг.
8. Нажмите на кнопку **Копировать в буфер обмена**, чтобы скопировать текст из текстового поля. Этот текст представляет собой двоичный объект данных (BLOB), который содержит параметры, необходимые для установления соединения между Сервером администрирования и управляемым устройством.

   > Объект BLOB действителен в течение 3 минут. Если срок его действия истек, сгенерируйте объект BLOB.
9. Запустите утилиту klsctunnel.

   Откроется окно утилиты.
10. Вставьте скопированный текст в текстовое поле.
11. Если вы используете прокси-сервер, установите флажок **Использовать прокси-сервер**, а затем укажите параметры подключения к прокси-серверу.
12. Нажмите на кнопку **Открыть порт**.

Совместный доступ к рабочему столу запускается в новом окне. Если вы хотите взаимодействовать с устройством, нажмите на значок меню ( ) в верхнем левом углу окна и выберите **Интерактивный режим**.

Срабатывание правил в режиме Интеллектуального обучения

В этом разделе представлена информация об обнаружениях, выполненных правилами Адаптивного контроля аномалий Kaspersky Endpoint Security для Windows на клиентских устройствах.

Правила обнаруживают аномальное поведение на клиентских устройствах и могут блокировать его. Если правила работают в режиме Интеллектуального обучения, они обнаруживают аномальное поведение и отправляют отчеты о каждом таком случае на Сервер администрирования Kaspersky Security Center Cloud Console. Эта информация хранится в виде списка в папке **Правила срабатываний в статусе Интеллектуальное обучение**, вложенной в папку **Хранилища**. 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.

Просмотр списка 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 **Операции → Хранилища**.
2. Перейдите по ссылке **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.

   - **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.

- **Имя пользователя**

  Имя пользователя клиентского устройства, запустившего процесс, который сгенерировал обнаружение.

- **Обработан**

  Дата обнаружения аномалии.

- **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).

Чтобы просмотреть свойства каждого элемента:

1. В главном окне приложения перейдите в раздел **Операции** → **Хранилища**.
2. Перейдите по ссылке **Правила срабатываний в статусе Интеллектуальное обучение**.
3. В открывшемся окне выберите нужный объект.
4. Перейдите по ссылке **Свойства**.

В открывшемся окне свойств объекта отображается информация выбранного элемента.

Вы можете подтвердить или добавить в исключения любой объект в списке, обнаруженный правилами Адаптивного контроля аномалий.

Чтобы подтвердить объект,

выберите один или несколько элементов в списке обнаружений и нажмите на кнопку **Подтвердить**.

Статус элементов будет изменен на **Подтверждается**.

Ваше подтверждение влияет на статистику, используемую правилами (подробную информацию см. в документации Kaspersky Endpoint Security для Windows).

Чтобы добавить объект в исключения,

выберите один или несколько элементов в списке обнаружений и нажмите на кнопку **Исключить**.

В результате запустится мастер добавления исключений. Следуйте далее указаниям мастера.

Если вы отклоните или подтвердите объект, он будет исключен из списка обнаружений после следующей синхронизации клиентского устройства с Сервером администрирования и больше не будет отображаться в списке.

Добавление исключений в правила Адаптивного контроля аномалий

Мастер добавления исключений позволяет добавлять исключения из правил Адаптивного контроля аномалий для Kaspersky Endpoint Security для Windows.

Чтобы запустить мастер добавления исключений в папке Адаптивный контроль аномалий:

1. В главном окне приложения перейдите в раздел **Операции → Хранилища → Правила срабатываний в статусе Интеллектуальное обучение**.
2. В открывшемся окне в контекстном меню одного или нескольких элементов в списке обнаружений нажмите на кнопку **Исключить**.

   За один раз можно добавить до 1000 исключений. Если вы выберете больше элементов и попытаетесь добавить их в исключения, появится сообщение об ошибке.

   В результате запустится мастер добавления исключений. Для продолжения работы мастера нажмите на кнопку **Далее**.

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

Исходно иерархия групп администрирования содержит только одну группу администрирования, которая называется **Управляемые устройства**. Вы можете добавлять устройства и подгруппы в состав группы **Управляемые устройства**.

Чтобы создать группу администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами → Иерархия групп**.
2. В иерархии выберите группу администрирования, которая должна включать новую группу администрирования.
3. Нажмите на кнопку **Добавить**.
4. В открывшемся окне введите имя группы и нажмите на кнопку **ОК**.

Новая группа администрирования, с указанным именем, появится в иерархии групп администрирования.

Приложение позволяет создавать структуру групп администрирования на основе структуры Active Directory или структуры доменной сети. Также вы можете создавать структуру групп из текстового файла.

Чтобы создать структуру групп администрирования:

1. В главном окне 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** и нажмите на имя нужной группы администрирования.
2. В открывшемся окне свойств перейдите на вкладку **Автоматическая установка**.
3. 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. Приложение применяет 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 нужно 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. В панели инструментов нажмите на кнопку **Переместить**.
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.

Политики и профили 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 Cloud Console предоставляет по одной политике для каждого приложения "Лаборатории Касперского" в группе администрирования. Политика имеет один из следующих статусов (см. таблицу ниже):

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.

- Вы можете активировать неактивную политику при возникновении определенного события. Например, в период вирусных атак можно включить параметры для усиленной антивирусной защиты.

- Политика может иметь дочерние политики.

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

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

Профиль политики – это именованное подмножество параметров политики, которые заменяют значения параметров политики. Профиль политики влияет на формирование эффективных параметров управляемого устройства. *Эффективные параметры* – это набор параметров политики, параметров профиля политики и параметров 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.

Вы не можете создать политику Сервера администрирования.

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:

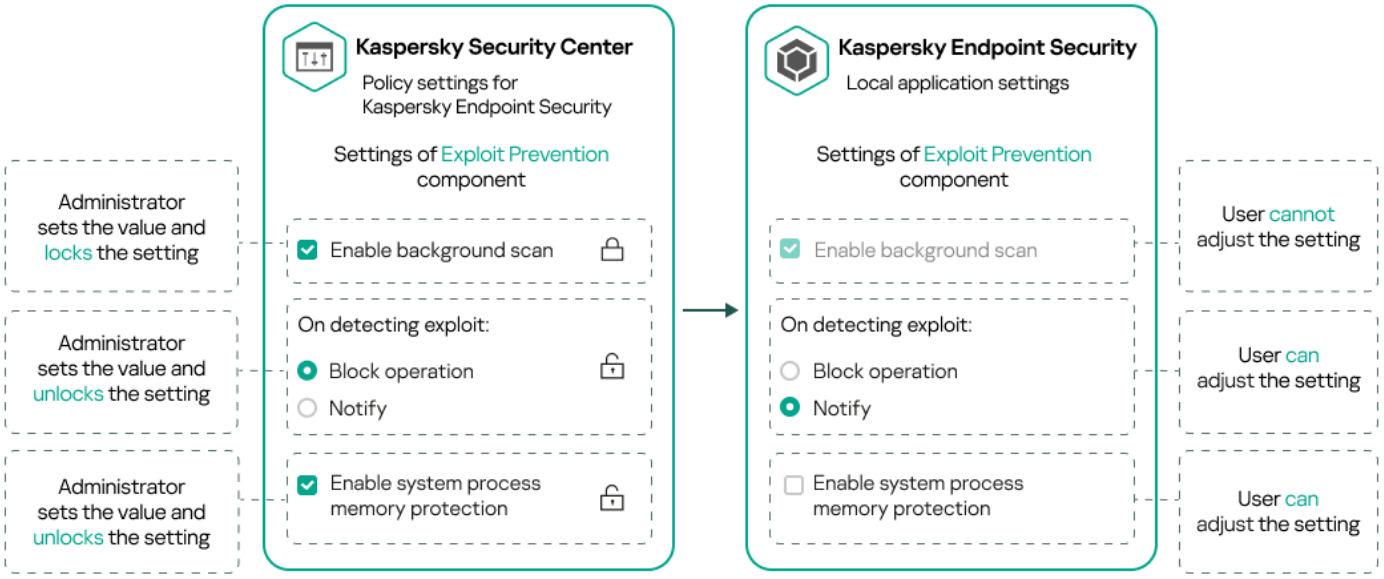
- Блокировка параметров для политики подгруппы администрирования.
- Блокировка параметров приложения "Лаборатории Касперского" на управляемом устройстве.

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

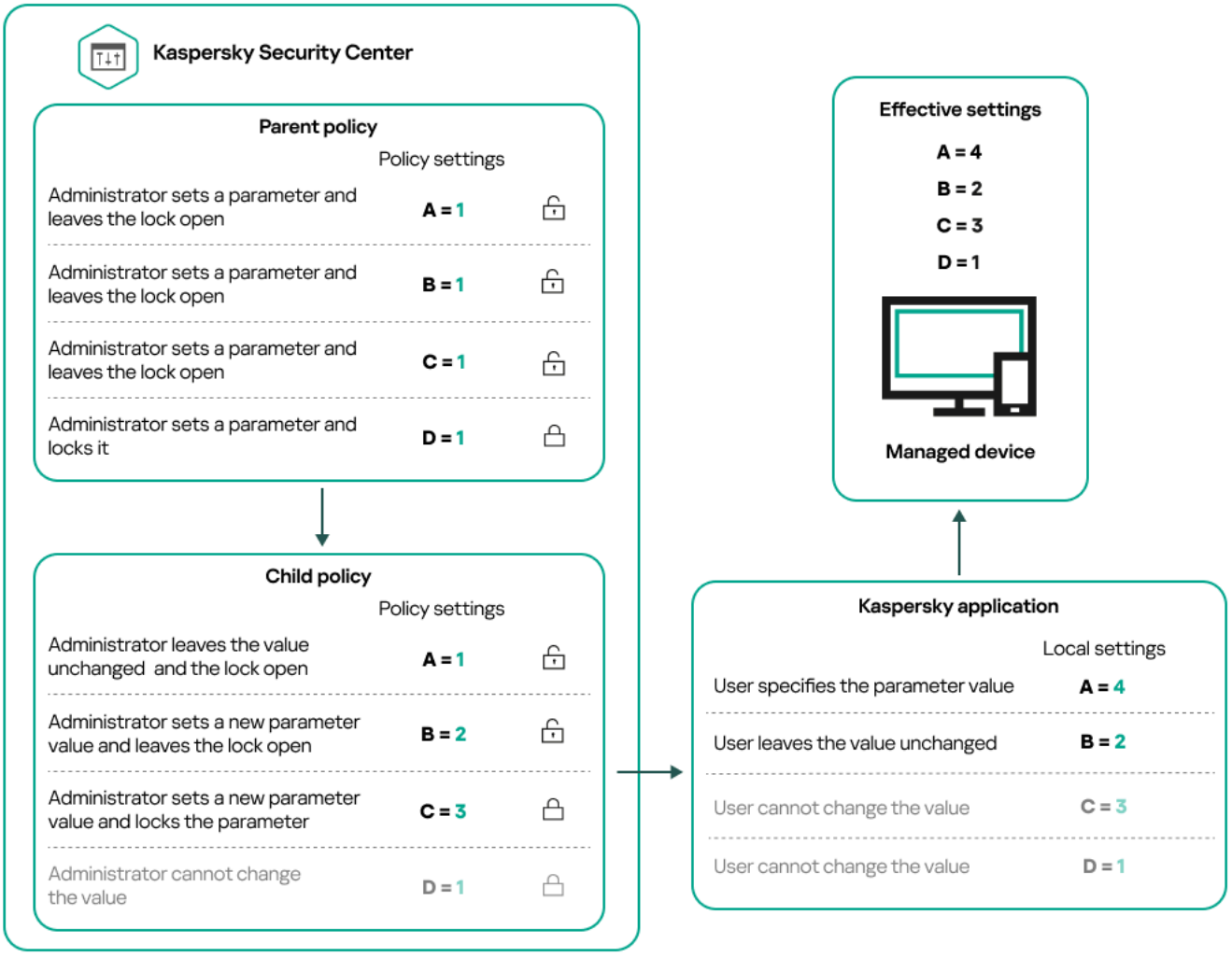
Если для разных устройств требуются разные параметры, вы можете объединить устройства в группы администрирования.

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).

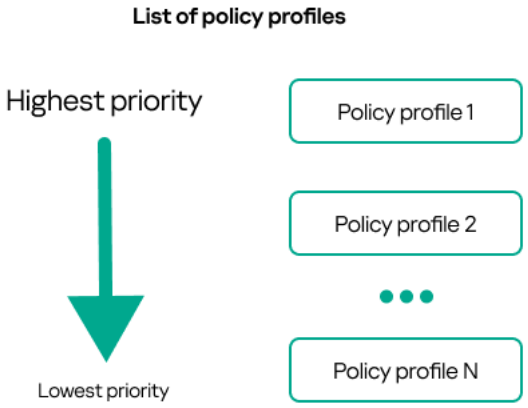


Иерархия политик

Профили политик в иерархии политик

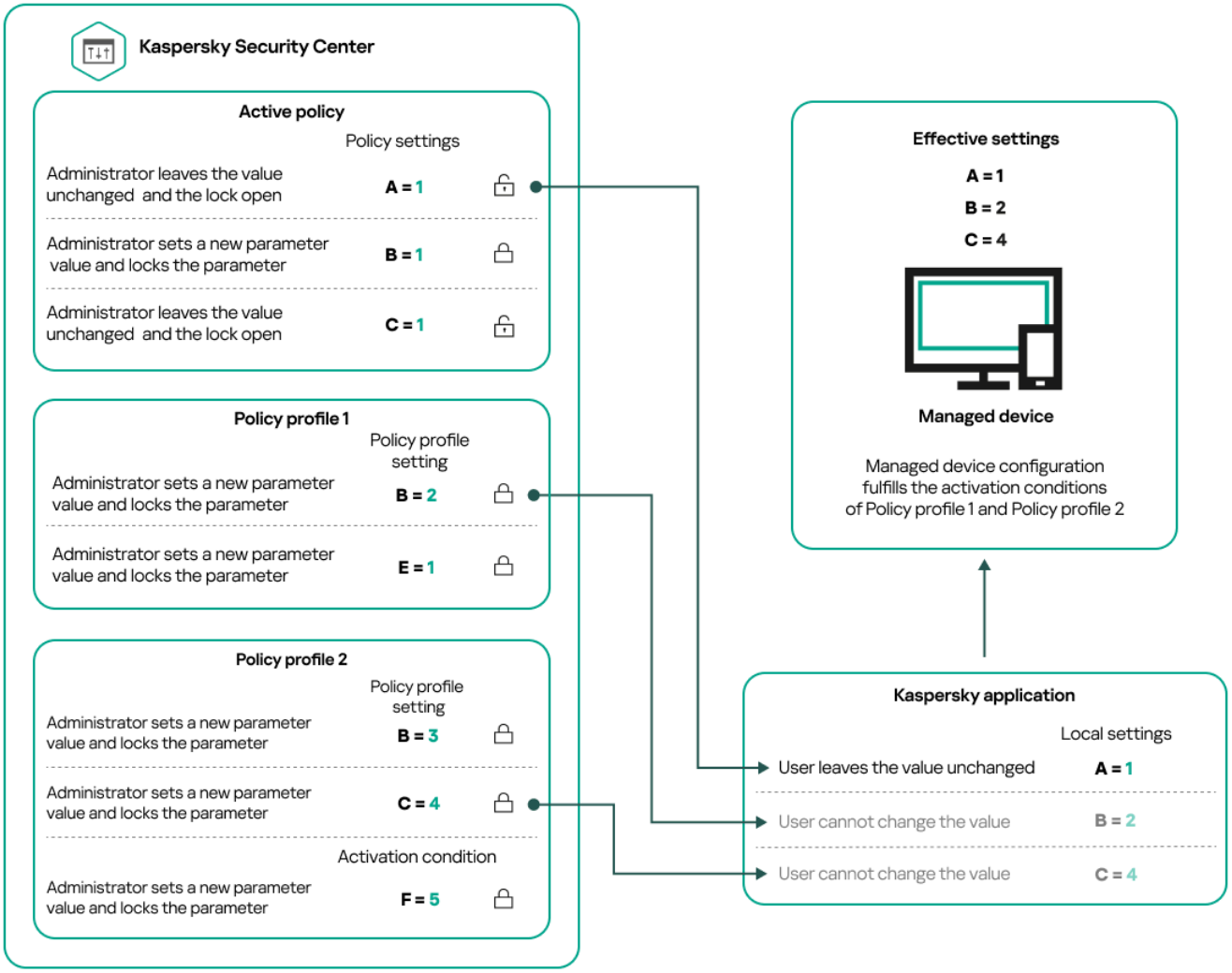
Профили политики имеют следующие условия назначения приоритета:

- 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).

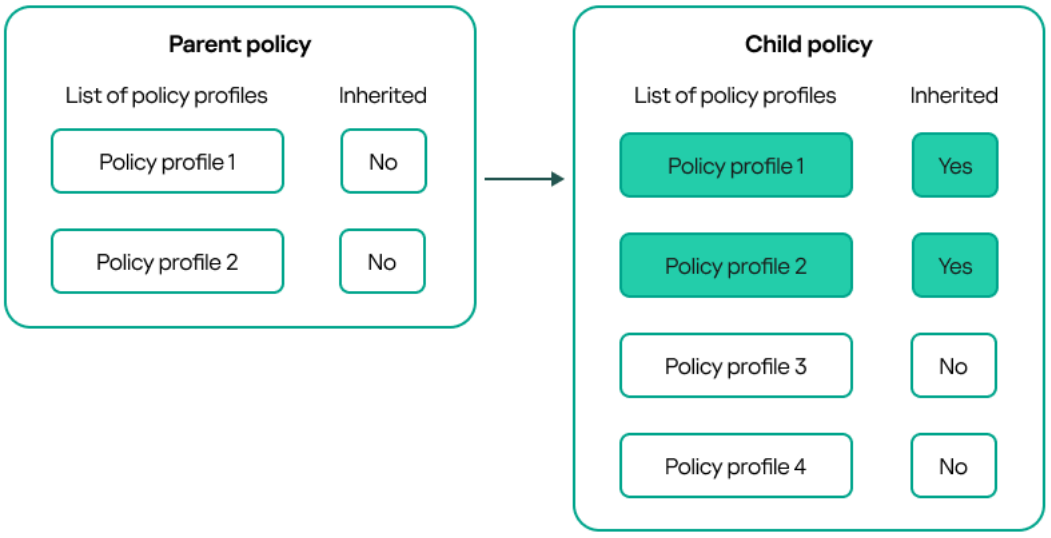


Конфигурация управляемого устройства соответствует условиям активации нескольких профилей политик

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.

> Вы не можете создать политику Сервера администрирования.

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. Чтобы перейти к группе администрирования, нажмите на ссылку с названием группы. По умолчанию последняя ссылка в пути неактивна. Также вы можете закрыть окно иерархии, нажав на кнопку **Скрыть иерархию**.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Выберите приложение**.
4. Выберите приложение, для которого требуется создать политику.

5. Нажмите на кнопку **Далее**.

   Откроется окно параметров новой политики на вкладке **Общие**.

6. При желании вы можете изменить следующие параметры политики, заданные по умолчанию: имя, состояние и наследование.

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.

   Параметры зависят от приложения, для которого вы создаете политику. Подробную информацию см. в следующих источниках:

   - Настройка Сервера администрирования
   - Параметры политики Агента администрирования
   - Документация 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.

В результате добавленная политика отображается в списке политик.

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
   - Документация Kaspersky Endpoint Security для Windows

   Подробнее о параметрах других приложений безопасности см. в документации к этим приложениям.

4. Нажмите на кнопку **Сохранить**.

   Отобразится уведомление: **Политика сохраняется и распространяется по иерархии Серверов администрирования**.

Если политика прошла проверку, отображается 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 просмотреть и изменить параметры политики, а затем повторить попытку. Если проблема продолжает сохраняться, обратитесь в Службу технической поддержки.

Изменения политики будут сохранены в свойствах политики и будут отображаться в разделе **История ревизий**.

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).

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**
  - **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:

  - **Хранить в базе данных Сервера администрирования в течение (сут)**
  - **Хранить в журнале событий ОС на устройстве**

- **Уведомления о событиях**

  Вы можете выбрать, хотите ли вы получать уведомления о событии по электронной почте.

  По умолчанию используются параметры уведомлений, указанные на вкладке свойств Сервера администрирования (например, адрес получателя). Вы можете изменить эти параметры на вкладке **Электронная почта**.

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.

Включение и выключение параметра наследования политики

Чтобы включить или выключить параметр наследования в политике:

1. Откройте требуемую политику.
2. Откройте вкладку **Общие**.
3. Включение или выключение наследования политики:
   - Если вы включили 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.
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 **ОК**, чтобы подтвердить операцию.

Политика (политики) и все ее профили скопированы в целевую группу администрирования. Каждая скопированная политика в целевой группе принимает статус **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

Если в целевой группе политик уже существует политика с именем, совпадающим с именем копируемой политики, к имени копируемой политики будет добавлено окончание вида (<следующий порядковый номер>), например: (1).

Перемещение политики

Вы можете перемещать политики из одной группы администрирования в другую. Например, вы хотите удалить одну группу администрирования, но использовать ее политики для другой группы администрирования. В этом случае вам может потребоваться, перед удалением старой группы администрирования, переместить политику из старой группы администрирования в новую.

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 **ОК**, чтобы подтвердить операцию.

   Если политика не унаследована из группы источника, она будет перемещена в целевую группу со всем профилями политики. Статус политики в целевой группе администрирования будет **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

   Если политика унаследована из группы источника, она останется в группе источника. Политика скопирована в целевую группу со всеми ее профилями. Статус политики в целевой группе администрирования будет **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

Если в целевой группе политик уже существует политика с именем, совпадающим с именем копируемой политики, к имени копируемой политики будет добавлено окончание вида (<следующий порядковый номер>), например: (1).

Экспорт политики

Kaspersky Security Center Cloud Console 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.
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 Cloud Console 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 имя новой импортированной политики идентично имени существующей политики, имя импортированной политики расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Просмотр диаграммы состояния применения политики

В Kaspersky Security Center Cloud Console 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.
3. В появившемся меню перейдите по ссылке **Результаты применения**.

   Откроется окно **Результат распространения <название политики>**.
4. В открывшемся окне **Результат распространения <название политики>** отображается **Описание статуса (если доступно)**.

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 панели справа перейдите по ссылке **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.

Принудительная синхронизация

Несмотря на то, что Kaspersky Security Center Cloud Console автоматически синхронизирует состояние, параметры, задачи и политики для управляемых устройств, в некоторых случаях требуется точно знать, выполнена ли синхронизация определенного устройства на данный момент.

Чтобы эта функция работала, необходимо включить параметр **Не разрывать соединение с Сервером администрирования** и/или использовать точку распространения в качестве push-сервера.

Синхронизация одного устройства

Чтобы осуществить принудительную синхронизацию между Сервером администрирования и управляемым устройством:

1. В главном окне приложения перейдите в раздел **Управление активами → Активы (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 → Активы (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. Чтобы перейти к группе администрирования, нажмите на ссылку с названием группы. 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 (...) и 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 вы можете 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 → Активы (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 программы, с выбранным разделом **Общие**, и отобразится дата и время доставки политики.

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.

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.

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.
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**.

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

Профиль политики отобразится в списке профилей политики.

Изменение профиля политики

Изменение профиля доступно только для политик Kaspersky Endpoint Security для Windows.

Чтобы изменить профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. На вкладке **Профили политики** нажмите на профиль политики, который вы хотите изменить.

   В результате откроется окно свойств профиля политики.

3. В окне свойств настройте параметры профиля:

   - Если необходимо, на вкладке **Общие** измените имя профиля политики и включите или выключите профиль.
   - Измените правила активации профиля политики.
   - Измените остальные параметры.

   Подробнее о параметрах приложений безопасности см. в документации к соответствующему приложению.

4. Нажмите на кнопку **Сохранить**.

Измененные параметры начнут действовать после синхронизации устройства с Сервером администрирования (если профиль политики активен) либо после выполнения правила активации (если профиль политики неактивен).

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 "≠").

      Обратите внимание, что список пользователей отфильтрован и отображаются владельцы устройств, которые являются внутренними пользователями.

      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 Cloud Console. 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 "≠").

      Обратите внимание, что список пользователей отфильтрован и отображаются владельцы устройств, которые являются внутренними пользователями.

Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать группу безопасности Kaspersky Security Center Cloud Console. 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:

- **Тег**

  В списке тегов задайте правило включения устройств в профиль политики, установив флажки нужным тегам.

  Вы можете добавить в список новые теги, введя их в поле над списком и нажав на кнопку **Добавить**.

  В профиль политики будут включены устройства, в описании которых есть все выбранные теги. Если флажки сняты, критерий не применяется. По умолчанию флажки сняты.

- **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.

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.

Шифрование и защита данных

Шифрование данных снижает риски непреднамеренной утечки информации в случае кражи/утери портативного устройства или жесткого диска, или при доступе к данным неавторизованных пользователей и приложений.

Шифрование поддерживают следующие приложения "Лаборатории Касперского":

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Mac

Вы можете отобразить или скрыть некоторые элементы интерфейса, связанные с управлением шифрованием, с помощью параметров пользовательского интерфейса.

Не рекомендуется включать шифрование в VDI.

Шифрование данных в Kaspersky Endpoint Security для Windows

Вы можете управлять технологией шифрования диска BitLocker на устройствах под управлением операционной системы Windows для серверов или рабочих станций.

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.

Вы управляете шифрованием, настраивая политики Kaspersky Endpoint Security для Windows в Kaspersky Security Center Cloud Console. Kaspersky Endpoint Security для Windows выполняет шифрование и расшифровку в соответствии с активной политикой. Подробные инструкции по настройке правил и описание особенностей шифрования см. в справке Kaspersky Endpoint Security для Windows.

Шифрование данных в Kaspersky Endpoint Security для Mac

Вы можете использовать шифрование FileVault на устройствах с операционными системами macOS. При работе с Kaspersky Endpoint Security для Mac вы можете включить или выключить это шифрование.

Шифрование настраивается путем определения политик Kaspersky Endpoint Security для Mac в Kaspersky Security Center Cloud Console. Kaspersky Endpoint Security для Mac выполняет шифрование и расшифровку в соответствии с активной политикой. Подробное описание функций шифрования см. в справке Kaspersky Endpoint Security для Mac.

Просмотр списка зашифрованных жестких дисков

В Kaspersky Security Center Cloud Console 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**.

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 раздел **Зашифрованные жесткие диски**, чтобы сформировать отчет о состоянии шифрования запоминающих устройств или отчет о правах доступа к зашифрованным жестким дискам.

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 для Windows не установлен на управляемом устройстве. После получения запроса вы можете создать файл ключа доступа и отправить его пользователю. Все варианты использования и подробные инструкции приведены в справке Kaspersky Endpoint Security для Windows.

Чтобы предоставить доступ к зашифрованному жесткому диску в автономном режиме:

1. Получите файл запроса доступа от пользователя (файл с расширением FDERTC). Следуйте инструкциям в справке Kaspersky Endpoint Security для Windows, чтобы сгенерировать файл в Kaspersky Endpoint Security для Windows.

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, соответствующий приложению "Лаборатории Касперского", которое использовалась для шифрования выбранного диска.

6. Следуйте инструкциям, приведенным в справке Kaspersky Endpoint Security для Windows (см. раскрывающиеся блоки в конце раздела).

После этого пользователь может использовать полученный файл для доступа к зашифрованному жесткому диску и чтения данных, хранящихся на диске.

Пользователи и роли пользователей

В этом разделе описана работа с пользователями и ролями пользователей, а также приведены инструкции по их созданию и изменению, назначению пользователям ролей и групп и связи профилей политики с ролями.

Об учетных записях пользователей

Kaspersky Security Center Cloud Console позволяет управлять учетными записями пользователей и группами учетных записей. 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 Cloud Console. Вы можете создавать учетные записи внутренних пользователей. Эти учетные записи используются только в Kaspersky Security Center Cloud Console.

Чтобы просмотреть таблицы учетных записей пользователей и групп безопасности:

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

2. Выберите вкладку **Пользователи** или **Группы**.

Откроется таблица пользователей или групп безопасности. По умолчанию открытая таблица фильтруется по столбцам **Тип учетной записи** и **Имеет назначенные роли**. В таблице показаны внутренние пользователи или группы, которым назначены роли.

Если вы хотите просмотреть таблицу только с учетными записями локальных пользователей, установите в фильтре **Тип учетной записи** критерий **Локальный**.

Если вы переключитесь на подчиненный Сервер администрирования версии 14.2 или ниже, а затем откроете список пользователей или групп безопасности, то открытая таблица будет отфильтрована только по столбцу **Тип учетной записи**. Фильтр по столбцу **Имеет назначенные роли** не будет применяться по умолчанию. Отфильтрованная таблица будет содержать всех внутренних пользователей или группы безопасности с назначенной ролью и без нее.

Добавление учетной записи внутреннего пользователя

В Kaspersky Security Center Cloud Console вы можете добавлять новых пользователей в рабочую область. Например, вы можете назначить добавленного пользователя владельцем устройства.

Чтобы добавить учетную запись внутреннего пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли → Пользователи и группы**.
2. На вкладке **Пользователи** нажмите **Добавить**.
3. В открывшемся окне **Добавить пользователей** введите адрес электронной почты пользователя, которого вы хотите добавить, и нажмите на кнопку **Далее**.
4. Просмотрите и измените данные пользователя.
5. Нажмите на кнопку **Готово**, чтобы сохранить изменения.

Учетная запись внутреннего пользователя будет добавлена и появится в списке пользователей.

Чтобы изменить информацию учетной записи внутреннего пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли → Пользователи и группы**.
2. В списке пользователей нажмите на учетную запись пользователя, которую требуется изменить.
3. В открывшемся окне измените необходимую информацию.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Чтобы разрешить добавленному внутреннему пользователю входить в Web Console и управлять рабочей областью, вы можете предоставить ему права администратора рабочей области в Kaspersky Security Center Cloud Console. Вы также можете удалить учетную запись внутреннего пользователя.

Удаление учетной записи внутреннего пользователя

Чтобы удалить учетную запись внутреннего пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли → Пользователи и группы**.
2. Установите флажок напротив пользователя, которого нужно удалить.
3. Нажмите на кнопку **Удалить**.
4. Подтвердите удаление.

Учетная запись внутреннего пользователя удалена и не может быть восстановлена.

Назначение администраторов рабочей области

В Kaspersky Security Center Cloud Console вы можете предоставить пользователям права администратора рабочей области. Администраторы рабочей области могут войти в Web Console и управлять рабочей областью.

Чтобы назначить администратора рабочей области:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы**.
2. На вкладке **Пользователи** нажмите на имя пользователя, которого вы хотите назначить администратором рабочей области.
3. В открывшемся окне включите переключатель **Администратор рабочей области**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Чтобы отозвать права администратора рабочей области, выключите переключатель **Администратор рабочей области**.

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 Cloud Console предоставляет доступ на основе ролей к функциям Kaspersky Security Center Cloud Console и к функциям управляемых приложений "Лаборатории Касперского".

Вы можете настроить права доступа к функциям приложения для пользователей Kaspersky Security Center Cloud Console 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 Cloud Console 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**.

Права доступа к функциям приложения

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 объ неза спи** пред ауди поль пред прав фун обла полу дост всем Реко пред прав круг кото для слу обя: Дос пред неза прав запр чте опр 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**. • Просмотрите журнал событий Kaspersky Event Log: **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 периметра. • Сводный отчет о типах установленных приложений. • Отчет о пользователях зараженных устройств. • Отчет о проблемах безопасности. • Отчет о событиях. • Отчет о работе точек распространения. • Отчет о подчиненных Серверах администрирования. • Отчет о событиях Контроля устройств. • Отчет об уязвимостях.	Отс

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
				• Отчет о запрещенных приложениях. • Отчет о работе Веб-Контроля. • Отчет о статусе шифрования управляемых устройств. • Отчет о статусе шифрования запоминающих устройств. • Отчет об ошибках шифрования файлов. • Отчет о блокировании доступа к зашифрованным файлам. • Отчет о правах доступа к зашифрованным устройствам. • 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.	Пар • • • •
Общие функции: **Развертывание приложений "Лаборатории Касперского"**	• **Управление патчами "Лаборатории Касперского".** • **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	Одобрить или отклонить установку патча: **Управление патчами "Лаборатории Касперского"**.	Отсутствует.	• Отчет об использовании лицензионных ключей виртуальным Сервером администрирования. • Отчет о версиях приложений "Лаборатории Касперского".	Инс паке "Лаб Кас

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
				• 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

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
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.** • **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Получение списка виртуальных Серверов администрирования: **Чтение**. • Получение информации о виртуальном Сервере администрирования: **Чтение**. • Создание, обновление или удаление виртуального Сервера администрирования: **Управление виртуальными Серверами администрирования**. • Перемещение виртуального Сервера администрирования в другую группу: **Управление виртуальными Серверами администрирования**. • Установка прав доступа к виртуальному Серверу администрирования: **Управление виртуальными Серверами администрирования**.	Отсутствует.	Отчет о результатах установки обновлений стороннего ПО.	Отс

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 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: **Инвентаризация оборудования**	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Получение или экспорт объектов инвентаризации оборудования: **Чтение**. • Добавление, установка или удаление объектов инвентаризации оборудования: **Запись**.	Отсутствует.	• Отчет о реестре оборудования. • Отчет об изменении конфигурации. • Отчет об оборудовании.	Отс
Управление системой: **Управление доступом в сеть**	• **Чтение.** • **Запись.**	• Просмотр параметров Cisco: **Чтение**. • Изменение параметров Cisco: **Запись**.	Отсутствует.	Отсутствует.	Отс
Управление системой: **Развертывание операционной системы**	• **Развертывание PXE-серверов.** • **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Развертывание PXE-серверов: **Развертывание PXE-серверов**. • Просмотр списка PXE-серверов: **Чтение**. • Запуск или остановка процесс установки на PXE-клиентах: **Выполнение**. • Управление драйверами для среды WinPE и образов операционной системы: **Запись**.	Создание инсталляционного пакета на основе образа ОС эталонного устройства.	Отсутствует.	Инс пак опе сис
Управление системой: **Системное администрирование**	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Просмотр свойства патчей сторонних производителей: **Чтение**. • Изменение свойства патчей сторонних производителей: **Запись**.	• Выполнение синхронизации обновлений Центра обновления Windows. • Установка обновлений Центра обновления Windows.	Отчет об обновлениях ПО.	Отс

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
			• Закрытие уязвимостей. • Установка требуемых обновлений и закрытия уязвимостей.		
Управление системой: **Удаленная установка**	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Просмотр Системного администрирования стороннего производителя на основе свойств инсталляционного пакета: **Чтение**. • Изменение Системного администрирования на основе свойств инсталляционного пакета: **Запись**.	Отсутствует.	Отсутствует.	Инст паке • •
Управление системой: **Инвентаризация приложений**	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	Отсутствует.	Отсутствует.	• Отчет об установленных приложениях. • Отчет об истории реестра приложений. • Отчет о состоянии групп лицензионных приложений. • Отчет о лицензионных ключах сторонних приложений.	Отс

Предопределенные роли пользователей

Роли пользователей, назначенные пользователям Kaspersky Security Center Cloud Console, предоставляют им набор прав доступа к функциям приложения.

Пользователям, которые были созданы на виртуальном Сервере, невозможно назначить роли на Сервере администрирования.

Вы можете использовать предопределенные роли пользователей с уже настроенным набором прав или создавать роли и самостоятельно настраивать необходимые права. Некоторые из предопределенных ролей пользователей, доступных в Kaspersky Security Center Cloud Console, могут быть связаны с определенными должностями, например, **Аудитор**, **Специалист по безопасности**, **Контролер** (эти роли присутствуют в Kaspersky Security Center Cloud Console начиная с версии 11). Права доступа этих ролей предварительно настраиваются в соответствии со стандартными задачами и обязанностями соответствующих должностей. В таблице ниже показано как роли могут быть связаны с определенными должностями.

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.** • **Обработка событий.** • **Иерархия Серверов администрирования.** • **Виртуальные Серверы администрирования.** • **Управление системой**: • **Подключения.** • **Инвентаризация оборудования.** • **Инвентаризация приложений.** Предоставляет права на **Чтение** и **Запись** в области **Общие функции: Управление ключами шифрования**.
Оператор Сервера администрирования	Предоставляет права на **Чтение** и **Выполнение** во всех следующих функциональных областях: • **Общие функции**: • **Базовая функциональность.** • **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.

Роль	Описание
Администратор установки приложений	Разрешает все операции в следующих функциональных областях: • **Общие функции**: • **Базовая функциональность.** • **Развертывание приложений "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**.
Оператор установки приложений	Предоставляет права на **Чтение** и **Выполнение** 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.** • Область Kaspersky Endpoint Security, включая все функции. Предоставляет права на **Чтение** и **Запись** в области **Общие функции: Управление ключами шифрования**.
Оператор Kaspersky Endpoint Security	Предоставляет права на **Чтение** и **Выполнение** во всех следующих функциональных областях: • **Общие функции: Базовая функциональность.** • Область Kaspersky Endpoint Security, включая все функции.
Главный администратор	Разрешает все операции в функциональных областях, *за исключением* следующих областей: **Общие функции**: • **Доступ к объектам независимо от их списков ACL.** • **Управление отчетами.** Предоставляет права на **Чтение** и **Запись** в области **Общие функции: Управление ключами шифрования**.

Роль	Описание
Главный оператор	Предоставляет права на **Чтение** и **Выполнение** (если применимо) во всех следующих функциональных областях: • **Общие функции**: • **Базовая функциональность.** • **Удаленные объекты.** • **Операции с Сервером администрирования.** • **Развертывание приложений "Лаборатории Касперского".** • **Виртуальные Серверы администрирования.** • **Управление мобильными устройствами: Общие.** • **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.** • **Управление мобильными устройствами: Общие.**
Оператор управления мобильными устройствами	Предоставляет права на **Чтение** и **Выполнение** в области **Общие функции**: **Базовая функциональность**. Предоставляет права на **Чтение** и **Отправление только информационных команд на мобильные устройства** в функциональной области: **Управление мобильными устройствами**: **Общие**.
Специалист по безопасности	Разрешает все операции в следующих функциональных областях: **Общие функции**: • **Доступ к объектам независимо от их списков ACL.** • **Управление отчетами.** Предоставляет права на **Чтение**, **Запись**, **Выполнение**, **Сохранение файлов с устройств на рабочую станцию администратора** и **Выполнение операций с выборками устройств** в области **Управление системой: Подключения**. Вы можете назначить эту роль сотруднику, который отвечает за IT-безопасность в вашей организации.
Главный специалист по безопасности	Предоставляет права на **Чтение** в области **Общие функции**: **Базовая функциональность**. Предоставляет права на **Чтение**, **Запись**, **Выполнение**, С**охранение файлов с устройств на рабочем месте администратора** и **Выполнение операций с выборками устройств** в области **Управление системой: Подключения**. Предоставляет права доступа к решению Kaspersky Endpoint Detection and Response Expert.
Пользователь Self Service Portal	Разрешает все операции в области **Управление мобильными устройствами: Self Service Portal**. Эта функция не поддерживается в версиях приложения Kaspersky Security Center 11 и выше.
Контролер	Предоставляет права на **Чтение** в области **Общие функции**: **Доступ к объектам независимо от их списков ACL** и **Общие функции**: **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).
Оператор Системного администрирования	Предоставляет права на **Чтение** и **Выполнение** (если применимо) в области **Общие функции**: **Базовая функциональность** и **Управление системой** (включая все функции).

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**.
   - **Управление активами → 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 **OK**.

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.

Назначение роли пользователю или группе безопасности

Чтобы назначить роли пользователю или группе безопасности:

1. В главном окне приложения перейдите в раздел U **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 шагам 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**.

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 пользователей и группы администрирования в область применения 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 пользователей, 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 или группы пользователей и выбранная группа администрирования добавлены в область применения 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 пользователей, которые требуется добавить в область применения роли.

7. Нажмите на кнопку **Назначить роль**, чтобы закрыть окно мастера.

8. Закройте окно свойств роли.

Выбранные пользователи или группы пользователей и выбранная группа администрирования добавлены в область применения 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, которых требуется добавить в область применения пользовательской роли, и нажмите на кнопку **Роли**.

   Вы не можете выбрать несколько пользователей или групп безопасности одновременно. Если вы выберете более одного объекта, кнопка **Роли** будет неактивна.

3. В окне **Роли** выберите пользовательскую роль, которую вы хотите назначить, и нажмите на кнопку **ОК**, чтобы сохранить 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 **ОК**.

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.

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 **Новая группа**.

3. В окне **Новая группа** укажите следующие параметры для новой группы безопасности:

   - **Имя**
   - **Описание**

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

Группа безопасности добавлена в список групп безопасности.

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.

Добавление учетных записей пользователей во внутреннюю группу

Учетные записи внутренних пользователей можно добавлять только во внутреннюю группу.

Чтобы добавить учетные записи пользователей в группу:

1. В главном окне 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.
3. Нажмите на кнопку **Назначить группу**.

4. В открывшемся окне **Назначить группу** выберите группу, в которую требуется добавить учетные записи пользователей.

5. Нажмите на кнопку **Назначить**.

   Учетные записи пользователей добавлены в группу. Также можно добавить внутренних пользователей в группу, используя параметры группы.

Удаление группы безопасности

Можно удалять только внутренние группы безопасности.

Чтобы удалить группу пользователей:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Группы**.

2. Установите флажок напротив группы пользователей, которую требуется удалить.

3. Нажмите на кнопку **Удалить** и подтвердите удаление в открывшемся окне.

   Группа пользователей удалена.

Настройка ADFS-интеграции

Чтобы разрешить пользователям, зарегистрированным в Active Directory (AD) вашей организации, входить в Kaspersky Security Center Cloud Console, вам необходимо настроить интеграцию со службами Active Directory Federation Services (AD FS).

Kaspersky Security Center Cloud Console поддерживает AD FS 3 (Windows Server 2016) или выше. AD FS должен быть опубликован и доступен в интернете. В качестве сертификата связи служба AD FS использует публичный доверенный сертификат.

Чтобы изменить параметры AD FS-интеграции, вам нужны права доступа для изменения прав пользователей.

Прежде чем продолжить, убедитесь, что вы выполнили опрос Active Directory.

Чтобы настроить AD FS-интеграцию:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры интеграции с AD FS**.

3. Скопируйте URL обратного вызова.

   Этот URL понадобится вам для настройки интеграции в Консоли управления AD FS.

4. В Консоли управления AD FS добавьте группу приложений, а затем добавьте приложение, выбрав шаблон **Server application** (названия элементов интерфейса Microsoft приведены на английском языке).

   Консоль управления AD FS генерирует идентификатор клиента для нового приложения. Идентификатор клиента понадобится вам для настройки интеграции в Kaspersky Security Center Cloud Console.

5. В качестве URI перенаправления укажите URL обратного вызова, который вы скопировали в окне свойств Сервера администрирования.

6. Создайте секрет клиента. Секрет клиента понадобится вам для настройки интеграции с Kaspersky Security Center Cloud Console.

7. Сохраните свойства добавленного приложения.

8. Добавьте приложение в созданную группу приложений. Выберите шаблон **Web API**.

9. На вкладке **Identifiers** в список **Relying party identifiers** добавьте идентификатор клиента серверного приложения, которое вы добавили ранее.

10. На вкладке **Client Permissions** в списке **Permitted scopes** выберите **allatclaims** и **openid**.

11. На вкладке **Issuance Transform Rules** добавьте правило, выбрав шаблон **Send LDAP Attributes as Claims**:

    a. Укажите название правила. Например, вы можете назвать его "Group SID".

    b. Выберите **Active Directory** в качестве хранилища атрибутов, а затем сопоставьте **Token-Groups as SIDs** в качестве атрибута LDAP с "Группа SID" в качестве типа исходящего утверждения.

12. На вкладке **Issuance Transform Rules** добавьте правило, выбрав **Send Claims Using a Custom Rule**:

    a. Укажите название правила. Например, ActiveDirectoryUserSID.

    b. В поле **Custom rule** укажите:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types =
("http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"), query =
";objectSID;{0}", param = c.Value);
```

13. В Kaspersky Security Center Cloud Console снова откройте раздел **Параметры интеграции с AD FS**.

14. Переведите переключатель в положение **Интеграция AD FS Включено**.

15. Перейдите по ссылке **Параметры** и укажите файл содержащий сертификат или несколько сертификатов федерального сервера.

16. Перейдите по ссылке **Параметры интеграции с AD FS** и укажите следующие параметры:

    - **URL издателя**

      URL сервера федерации, работающего в вашей организации.

В частности, Kaspersky Security Center Cloud Console добавляет '/.well-known/openid-configuration' к URL эмитента и пытается открыть полученный URL (issuer_URL/.well-known/openid-configuration), чтобы узнать конфигурацию эмитента автоматически.

- **Идентификатор клиента**

  Идентификатор клиента, который сервер федерации генерирует для идентификации Kaspersky Security Center Cloud Console. Вы можете найти идентификатор клиента в консоли управления AD FS в окне свойств серверного приложения, соответствующего Kaspersky Security Center Cloud Console.

- **Секрет клиента**

  Вы генерируете секрет клиента в консоли управления AD FS, когда указываете свойства серверного приложения, которое соответствует Kaspersky Security Center Cloud Console.

- **Доменная аутентификация пользователей**

  Участники выбранного вами домена смогут входить в Kaspersky Security Center Cloud Console, используя свои доменные учетные данные. Доменные имена появятся в списке после завершения опроса сети.

- **Имя поля для SID пользователя в идентификаторе токена**

  Имя поля, которое ссылается на идентификатор безопасности (SID) пользователя в токене идентификатора. Название поля необходимо для идентификации пользователя в Kaspersky Security Center Cloud Console. По умолчанию это поле в токене идентификатора называется 'primarysid'.

- **Имя поля для массива SID групп пользователей в идентификаторе токена**

  Имя поля, которое относится к массиву SID групп безопасности Active Directory, в которые входит пользователь. По умолчанию это поле в идентификаторе токена называется 'groupsid'.

17. Сохраните параметры.

Интеграция с AD FS завершена. Чтобы войти в Kaspersky Security Center Cloud Console с учетными данными AD, используйте ссылку в разделе **Параметры интеграции с AD FS** (**Ссылка для входа в Kaspersky с AD FS**).

После входа в Kaspersky Security Center Cloud Console с учетными данными AD распространяются следующие ограничения:

- Раздел **Data Discovery** недоступен в главном меню.
- Элемент **Управление учетной записью** недоступен в верхней панели.
- Вы не можете переключаться между рабочими областями.

При первом входе в Kaspersky Security Center Cloud Console через AD FS, консоль может реагировать с задержкой.

Настройка интеграции с Microsoft Entra ID

Вам необходимо настроить интеграцию с Microsoft Entra ID, чтобы пользователи вашей организации могли входить в Kaspersky Security Center Cloud Console под учетными данными Microsoft Entra ID.

Интеграция с Microsoft Entra ID доступна только для главного Сервера администрирования. Вы не можете настроить интеграцию для подчиненных или виртуальных Серверов администрирования.

Настройка параметров интеграции

Чтобы настроить интеграцию с Microsoft Entra ID:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Microsoft Entra ID**.

3. Включите переключатель **Интеграция с Microsoft Entra ID**.

4. Скопируйте ссылки из следующих полей:

   - **URL обратного вызова**
   - **Веб-адрес выхода из переднего канала**

     Эти адреса понадобятся вам для регистрации Kaspersky Security Center Cloud Console в тенанте Microsoft Entra ID.

   - **Веб-адрес входа**

     Этот URL понадобится вам, чтобы пользователи могли входить в рабочую область Kaspersky Security Center Cloud Console под своими учетными данными Microsoft Entra ID после завершения интеграции с Microsoft Entra ID.

5. Войдите в Microsoft Entra Admin Center и выберите тенант своей организации.

   У вас должна быть роль глобального администратора или администратора приложения в тенанте.

6. В главном меню выберите **Identity** → **Applications** → **App registrations** и нажмите на кнопку **New registration**.

7. В открывшемся окне выполните одно из следующих действий:

   - Укажите имя приложения Kaspersky Security Center Cloud Console.
   - В разделе **Supported account types** выберите параметр **Accounts in this organizational directory only (<tenant_name> only - Single tenant)**.
   - В разделе **Redirect URI** выберите в раскрывающемся списке **Web** и введите URL обратного вызова, который вы скопировали в Kaspersky Security Center Cloud Console на шаге 4.

8. Нажмите на кнопку **Register**.

   Приложение Kaspersky Security Center Cloud Console зарегистрировано в Microsoft Entra ID, и открывается страница обзора приложения.

9. При необходимости добавьте Kaspersky Security Center Cloud Console в список приложений.

   Пользователи смогут открыть приложение Kaspersky Security Center Cloud Console, нажав на его название в списке приложений в Мои приложения и Office 365 Launcher без использования веб-адреса для входа.

10. Скопируйте **Application (client) ID** и **Directory (tenant) ID** и сохраните их любым удобным способом.

    Эти идентификаторы понадобятся вам при заполнении обязательных полей в Kaspersky Security Center Cloud Console на шаге 14.

11. В меню приложения Kaspersky Security Center Cloud Console перейдите в раздел **Authentication** и введите URL, которые вы скопировали из Kaspersky Security Center Cloud Console на шаге 4:

    - В разделе **Web** нажмите на кнопку **Add URI** и введите URL для входа.
    - В разделе **Front-channel logout URL** введите URL выхода из основного канала.

12. В меню приложения Kaspersky Security Center Cloud Console перейдите в раздел **Certificates & secrets** и выполните следующие действия:

    a. Перейдите на вкладку **Client secrets** и нажмите на кнопку **New client secret**.

    b. В открывшемся окне укажите любое описание секрета клиента и выберите период, по истечении которого срок действия секрета истечет.

    > Рекомендуется любым удобным способом скопировать дату, после которой истекает срок действия секрета, чтобы своевременно изменять секреты.

    a. Нажмите на кнопку **Добавить**.

    Созданный секрет отображается на вкладке **Client secrets**.

    b. Скопируйте информацию из столбца **Value**.

    > Рекомендуется скопировать информацию сразу после создания секрета клиента.

13. В меню приложения Kaspersky Security Center Cloud Console перейдите в раздел **Token configuration** и выполните следующие действия:

    - Добавьте необязательное утверждение **onprem_sid**:

        a. Нажмите на кнопку **Add optional claim**.

        b. В открывшемся окне выберите тип токена **ID** и в столбце **Claim** установите флажок рядом с **onprem_sid**.

        c. Нажмите на кнопку **Добавить**.

        Необязательное утверждение **onprem_sid** отображается на странице **Optional claims**.

    - Добавьте необязательное утверждение **preferred_username**:

        a. Нажмите на кнопку **Add optional claim**.

        b. В открывшемся окне выберите тип токена **Access** и в столбце **Claim** установите флажок рядом с **preferred_username**.

        c. Нажмите на кнопку **Добавить**.

        Необязательное утверждение **preferred_username** отображается на странице **Optional claims**.

14. В меню приложения Kaspersky Security Center Cloud Console перейдите в раздел **API permissions** и добавьте разрешения:

    - **User.Read.All**
    - **User.Export.All**
    - **GroupMember.Read.All**
    - **Directory.Read.All**

    Чтобы добавить разрешения:

    a. Нажмите на кнопку **Add a permission** и выберите вкладку **Microsoft API**.

    b. Выберите **Microsoft Graph** → **Application permissions** и выберите разрешение, которое вы хотите добавить.

    c. Нажмите на кнопку **Add permission**.

    Четыре разрешения добавлены и отображаются на странице **Configured permissions**.

    d. Нажмите кнопку **Предоставить согласие администратора для <tenant_name>**, а затем в открывшемся окне нажмите **Да**, чтобы подтвердить предоставление согласия на добавленные вами разрешения.

15. Вернитесь в Kaspersky Security Center Cloud Console и на вкладке **Общие** заполните следующие обязательные поля:

    - **Идентификатор тенанта**. Значение поля **Directory (tenant) ID**, которое вы копируете на шаге 10.
    - **Идентификатор клиента**. Значение поля **Идентификатор приложения (клиента)**, которое вы копируете на шаге 10.
    - **Секрет клиента**. Значение, которое вы копируете на шаге 12.

16. Нажмите на кнопку **Проверить подключение**, чтобы проверить правильность параметров, а затем после отображения статуса **Подключено** нажмите на кнопку **Сохранить**.

Параметры интеграции сохранены, интеграция с Microsoft Entra ID настроена.

Проверка добавления пользователей

После настройки интеграции с Microsoft Entra ID необходимо выполнить следующие действия:

1. В главном окне приложения Kaspersky Security Center Cloud Console перейти в раздел **Пользователи и роли → Пользователи и группы**, чтобы убедиться, что пользователи и группы из Microsoft Entra ID добавлены в Kaspersky Security Center Cloud Console.

   Если пользователи и группы в вашем тенанте Microsoft Entra ID синхронизированы из Active Directory вашей организации и настроен опрос Active Directory, то пользователи и группы уже добавлены в Kaspersky Security Center Cloud Console в результате опроса Active Directory.

   Иначе вам необходимо включить и запустить опрос Microsoft Entra ID, чтобы добавить пользователей и группы из вашего тенанта Microsoft Entra ID в Kaspersky Security Center Cloud Console.

2. Назначить необходимые роли пользователям и группам.

   При назначении ролей пользователю на виртуальном Сервере администрирования в главном окне приложения перейдите в раздел **Пользователи и роли → Пользователи и группы** и выберите вкладку **Пользователи**. Если вы выберете вкладку **Группы** и назначите роли группе, членом которой является пользователь, пользователь не сможет войти в Kaspersky Security Center Cloud Console.

3. Отправить пользователям URL для входа, который вы скопировали на шаге 4. Они будут вводить этот URL для **входа в рабочую область Kaspersky Security Center Cloud Console, используя свои учетные данные Microsoft Entra ID**.

   Когда пользователь выходит из учетной записи Microsoft Entra ID, которую он использовал для аутентификации в Kaspersky Security Center Cloud Console, и приложение Kaspersky Security Center Cloud Console открыто на другой вкладке или в другом окне того же браузера, этот сеанс также заканчивается для Kaspersky Security Center Cloud Console и пользователь автоматически выходит из консоли.

   Если Kaspersky Security Center Cloud Console открыта в другом браузере или на других устройствах, сеанс продолжается, когда пользователь выходит из учетной записи Microsoft Entra ID.

Чтобы войти в Kaspersky Security Center Cloud Console с учетными данными Microsoft Entra ID, пользователи должны иметь возможность войти в свою учетную запись Microsoft Entra ID.

Ограничения

После входа в Kaspersky Security Center Cloud Console с учетными данными Microsoft Entra ID распространяются следующие ограничения:

- Раздел **Data Discovery** недоступен в главном меню.
- Элемент **Управление учетной записью** недоступен в верхней панели.
- Вы не можете переключаться между рабочими областями.

Включение опроса Microsoft Entra ID

Вам нужно включить опрос Microsoft Entra ID, чтобы добавить пользователей из Microsoft Entra ID в Kaspersky Security Center Cloud Console.

Чтобы включить опрос Microsoft Entra ID:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Microsoft Entra ID**.
3. В разделе **Обнаружение пользователей** включите переключатель **Опрос Microsoft Entra ID**.
4. Если вы хотите изменить расписание опроса по умолчанию, нажмите на кнопку **Параметры расписания**, укажите период и время опроса в открывшемся окне и нажмите на кнопку **Сохранить**.

   Опрос Microsoft Entra ID будет выполняться в соответствии с настроенным расписанием.

5. Если вы хотите запустить опрос Microsoft Entra ID немедленно, нажмите на кнопку **Запустить сейчас**.

   Начнется загрузка пользователей. Когда пользователи загрузятся, опрос Microsoft Entra ID завершится.

6. Нажмите на кнопку **Сохранить**.

Опрос Microsoft Entra ID завершен, пользователи из Microsoft Entra ID добавлены в Kaspersky Security Center Cloud Console.

Добавление Kaspersky Security Center Cloud Console в список приложений

Вы можете разрешить пользователям открывать приложение Kaspersky Security Center Cloud Console, нажав по его названию в списке приложений, не вводя веб-адрес для входа. Список приложений доступен в My Apps и в Office 365 Launcher.

Чтобы добавить Kaspersky Security Center Cloud Console в список приложений:

1. В главном меню центра администрирования Microsoft Entra перейдите в раздел **Identity** → **Applications** → **App registrations**, после чего на вкладке **All applications** выберите приложение Kaspersky Security Center Cloud Console, которое вы ранее зарегистрировали в Microsoft Entra ID.

2. В меню Kaspersky Security Center Cloud Console перейдите в раздел **Branding & properties** и выполните следующие действия:

   a. В поле **Home page URL** введите веб-адрес для входа.

   b. При необходимости в поле **Upload new logo** добавьте изображение, которое будет использоваться в качестве значка приложения в списке приложений.

   c. Нажмите на кнопку **Сохранить**.

3. В главном меню Центра администрирования Microsoft Entra перейдите в раздел **Identity** → **Applications** → **Enterprise applications** и выберите Kaspersky Security Center Cloud Console.

   Откроется страница обзора приложения.

4. В меню Kaspersky Security Center Cloud Console перейдите в раздел **Properties** и выполните следующие действия:

   a. Установите для следующих параметров значение **Да**:

   - **Разрешено ли пользователям входить в систему?**

     Это действие необходимо, только если по умолчанию для параметра не задано значение **Да**.

   - **Видны пользователям?**

   b. Нажмите на кнопку **Сохранить**.

5. В меню Kaspersky Security Center Cloud Console перейдите в раздел **Users and groups** и выполните следующие действия:

   a. Нажмите на кнопку **Add user/group** и перейдите по ссылке **Users and groups**.

   b. В открывшемся окне выберите пользователей и группы и нажмите на кнопку **Save**.

   Окно закрыто.

   c. Нажмите на кнопку **Назначить**.

Приложение Kaspersky Security Center Cloud Console доступно в My Apps и Office 365 Launcher для выбранных пользователей. Пользователи могут открыть приложение Kaspersky Security Center Cloud Console, нажав на его название в списке, без ввода веб-адреса для входа.

Назначение пользователя владельцем устройства

Информацию о назначении пользователя владельцем мобильного устройства см. в справке Kaspersky Security для мобильных устройств.

Чтобы назначить пользователя владельцем устройства:

1. 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 **ОК**.

Выбранное устройство добавляется в список устройств, назначенных пользователю.

Также можно выполнить эту операцию в группе **Управление активами → Активы (Устройства)**, выбрав имя устройства, которое вы хотите назначить, и перейдя по ссылке **Сменить владельца устройства**.

Назначение пользователя владельцем устройства Linux после установки Агента администрирования

Чтобы разрешить пользователю зарегистрироваться в качестве владельца устройства Linux:

1. В Kaspersky Security Center Cloud Console перейдите в раздел **Обнаружение устройств и развертывание → Развертывание и назначение → Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов.

2. Нажмите на инсталляционный пакет Агента администрирования.

   Отобразится окно свойств инсталляционного пакета.

3. В открывшемся окне свойств инсталляционного пакета перейдите на вкладку **Параметры → Дополнительно**.

4. В разделе **Регистрация пользователя в качестве владельца устройства (только для Linux)** включите параметр **Разрешить запуск утилиты регистрации 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.

Пользователь зарегистрирован как владелец устройства.

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 Kaspersky Security Center Cloud 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.

Добавление описания ревизии

Вы можете добавить описание для ревизии, чтобы в дальнейшем было проще найти необходимую ревизию в списке.

Чтобы добавить описание ревизии:

1. В окне свойств объекта перейдите на вкладку **История ревизий**.
2. В списке ревизий объекта выберите ревизию, для которой нужно добавить описание.
3. Нажмите на кнопку **Изменить описание**.

   Откроется окно **Описание**.
4. В окне **Описание** введите текст описания ревизии.

   По умолчанию описание ревизии объекта не заполнено.
5. Сохраните описание ревизии.

Описание добавлено для ревизии объекта.

Откат изменений объекта к предыдущей ревизии

В случае необходимости вы можете откатить изменения объекта. Например, вам может понадобиться вернуть параметры политики к состоянию на определенную дату.

Чтобы откатить изменения объекта:

1. В окне свойств объекта перейдите на вкладку **История ревизий**.
2. В списке ревизий объекта выберите номер ревизии, 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.

Просмотр и сохранение ревизии политики

Kaspersky Security Center Cloud Console позволяет просмотреть, какие изменения были внесены в политику за определенный период, и сохранить информацию об этих изменениях в файле.

Просмотр и сохранение ревизии политики доступны, если соответствующий веб-плагин управления поддерживает эту функцию.

Чтобы просмотреть ревизию политики:

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

   Если размер ревизии превышает 10 МБ, просмотреть ее с помощью Kaspersky Security Center Cloud 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. 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).

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).

Чтобы просмотреть ревизию 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 панели выполните следующие действия:

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 вашей Kaspersky Security Center Cloud 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.

Для политик Kaspersky Endpoint Security для Windows и Kaspersky Endpoint Security для Mac отчет о сравнении ревизий не будет содержать информацию о профилях политик.

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 клиентских устройствах.

Участвуя в программе KSN, вы соглашаетесь в автоматическом режиме предоставлять в "Лабораторию Касперского" информацию о работе приложений "Лаборатории Касперского", установленных на клиентских устройствах, находящихся под управлением Kaspersky Security Center Cloud Console. 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.

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 или при обновлении Сервера администрирования с предыдущей версии. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с предыдущей версией Положения о KSN, которую вы приняли ранее.

Когда KSN включен, Kaspersky Security Center Cloud Console проверяет доступность серверов KSN. Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы. Это необходимо, чтобы убедиться, что уровень безопасности поддерживается для управляемых устройств.

Клиентские устройства, находящиеся под управлением Сервера администрирования, взаимодействуют с KSN при помощи службы прокси-сервера KSN. Служба прокси-сервера KSN предоставляет следующие возможности:

- Клиентские устройства могут выполнять запросы к KSN и передавать в KSN информацию, даже если они не имеют прямого доступа в интернет.
- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентским устройством запрошенной информации.

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 (ksnproxy).

Включение и отключение KSN

Чтобы включить KSN:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры KSN**.

3. Переведите переключатель в положение **Использовать Kaspersky Security Network Включено**.

   KSN включен.

   Если переключатель включен, клиентские устройства будут передавать результаты установки патчей в "Лабораторию Касперского". Включая переключатель, вам нужно прочитать и принять условия Положения о KSN.

4. Нажмите на кнопку **Сохранить**.

Чтобы выключить KSN:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры KSN**.

3. Переведите переключатель в положение **Использовать Kaspersky Security Network Выключено**.

   KSN выключен.

   Если переключатель выключен, клиентские устройства не будут передавать результаты установки патчей в "Лабораторию Касперского".

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 **Параметры 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 было обновлено, оно автоматически отображается при открытии Kaspersky Security Center Cloud Console. 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. Вы можете просмотреть и принять обновленное Положение о KSN 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 KSN. Управляемое устройство работает как прокси-сервер KSN, если на нем запущена служба ksnproxy. Вы можете проверить включить или выключить эту службу на устройстве локально.

Вы можете назначить устройство с операционной системой Windows или Linux в качестве точки распространения. Способ проверки точки распространения зависит от операционной системы этой точки распространения.

Чтобы проверить, работает ли точка распространения с операционной системой Windows как прокси-сервер KSN:

1. На устройстве, которое выполняет роль точки распространения, в Windows откройте окно **Службы** (**Все 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.

Чтобы проверить, работает ли точка распространения с операционной системой Linux как прокси-сервер KSN:

1. На устройстве, выполняющем роль точки распространения, отобразится список запущенных процессов.

2. В списке запущенных процессов проверьте запущен ли процесс `/opt/kaspersky/ksc64/sbin/ksnproxy`.

Если процесс `/opt/kaspersky/ksc64/sbin/ksnproxy` запущен, то Агент администрирования на устройстве участвует в Kaspersky Security Network и работает как прокси-сервер KSN для управляемых устройств, входящих в область действия точки распространения.

Удаление объектов

Вы можете удалять следующие объекты:

- политики;
- задачи;
- инсталляционные пакеты;
- виртуальные Серверы администрирования;
- пользователей;
- группы безопасности;
- группы администрирования.

Когда вы удаляете объект, информация об этом записывается в базу данных. Срок хранения информации 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 программа 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 Cloud Console 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 шифрования диска BitLocker. 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 устройство (или 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.

  Чтобы расшифровать диск 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.

> 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 Cloud Console обнаружит устройство во время опроса сети и снова добавит его в группу Нераспределенные устройства. Поэтому удалять устройство вручную целесообразно только в том случае, если оно невидимо для Сервера администрирования.

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 Cloud Console 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. Это обслуживание обеспечит постоянную защиту управляемых устройств от различных угроз, включая вирусы, сетевые атаки и фишинговые атаки.

Существует несколько схем, которые вы можете использовать для установки обновлений компонентов Kaspersky Security Center Cloud Console и приложений безопасности. Выберите одну или несколько схем, которые лучше всего соответствуют требованиям вашей сети.

Сценарий ниже описывает схему обновления, которая подразумевает загрузку обновлений в хранилища точек распространения. Если у управляемых устройств нет соединения с точками распространения, рассмотрите возможность обновления баз, модулей приложений и приложений "Лаборатории Касперского" вручную или напрямую с серверов обновлений "Лаборатории Касперского".

После завершения этого сценария вы получите следующие результаты:

- Компоненты Kaspersky Security Center Cloud Console обновлены автоматически либо только тогда, когда вы устанавливаете обновлениям статус *Одобрено*.
- Приложения безопасности, базы и модули приложений "Лаборатории Касперского" обновлены в соответствии с расписанием. По умолчанию приложения безопасности "Лаборатории Касперского" устанавливают только те обновления, которые вы одобрили.

Вы можете настроить процесс обновления для загрузки и установки обновлений любым из двух способов:

- Автоматически

  В этом случае вам нужно выполнить этот только сценарий один раз. Вам нужно будет настроить расписание задачи *Загрузка обновлений в хранилища точек распространения* (если есть), задачи Обновление для приложений безопасности "Лаборатории Касперского" и сохранить параметры обновления по умолчанию в свойствах Агента администрирования.

- Вручную

  Вы можете настроить процесс обновления так, чтобы вручную запускать задачу *Загрузка обновлений в хранилища точек распространения* и задачу Обновление для приложений безопасности "Лаборатории Касперского". Вы также можете настроить Агент администрирования на установку обновлений для компонентов Kaspersky Security Center Cloud Console только в том случае, если вы устанавливаете статус обновлениям *Одобрено*.

Предварительные требования

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 Cloud Console. После выполнения этого сценария назначено нужное количество точек распространения в соответствии с количеством управляемых устройств и топологией сети.

2. Созданы и настроены все необходимые политики, профили политик и задачи в соответствии со сценарием настройки защиты сети.

Этапы

Настройка регулярного обновления баз и приложений "Лаборатории Касперского" состоит из следующих этапов:

1. **Создание задачи загрузки обновлений в хранилища точек распространения**

   Создание задачи *Загрузка обновлений в хранилища точек распространения*. После запуска этой задачи Kaspersky Security Center Cloud Console загружает обновления на точки распространения непосредственно с серверов обновлений "Лаборатории Касперского".

   Инструкция: Создание задачи загрузки обновлений в хранилища точек распространения

2. **Настройка точек 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, могут загружать обновления только из локального ресурса или напрямую с серверов обновлений "Лаборатории Касперского".

   Если вы хотите, чтобы управляемые устройства получали обновления только от точек распространения, включите параметр **Распространять файлы только через точки распространения** в политике Агента администрирования.

3. **Оптимизация процесса с использованием загрузки файлов различий (если требуется)**

   Включение этой функции приводит к уменьшению трафика между точками распространения и управляемыми устройствами. Чтобы использовать эту функцию, включите параметр **Скачать файлы различий** в свойствах задачи *Загрузка обновлений в хранилища точек распространения*.

   Инструкция: Использование файлов различий для обновления баз и модулей приложений "Лаборатории Касперского"

4. **Определение обновлений для установки**

По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Измените статус на *Одобрено* или *Отклонено*, чтобы определить, следует ли устанавливать это обновление на сетевые устройства. Одобренные обновления всегда устанавливаются. Неопределенные обновления могут быть установлены только на Агенте администрирования и других компонентах Kaspersky Security Center Cloud Console в соответствии с параметрами политики Агента администрирования. Обновления, которым вы установили статус *Отклонено*, не устанавливаются на управляемые устройства.

Инструкции:

- О статусах обновлений
- Одобрение и отклонение обновлений программного обеспечения

5. **Настройка автоматической установки обновлений и патчей для компонентов Kaspersky Security Center Cloud Console**

   По умолчанию загруженные обновления и патчи для Агента администрирования и других компонентов Kaspersky Security Center Cloud Console устанавливаются автоматически. Если вы оставили включенным параметр **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"** в свойствах Агента администрирования, тогда все обновления будут установлены автоматически после их загрузки в хранилище (или несколько хранилищ). Если флажок снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрен*.

   Инструкция: Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center Cloud Console

6. **Настройка автоматической установки обновлений для приложений безопасности**

   Создайте задачу "Обновление" для управляемых приложений, чтобы обеспечить своевременное обновление приложений, модулей приложений и баз данных "Лаборатории Касперского", в том числе антивирусных баз. Рекомендуется при настройке расписания задачи выбрать вариант **При загрузке обновлений в хранилище**. Это обеспечит установку новых обновлений как можно раньше.

   По умолчанию обновления для управляемых приложений устанавливаются только после изменения статуса обновления на *Одобрено*. Для Kaspersky Endpoint Security для Windows вы можете изменить параметры обновления в задаче Обновление.

   Если обновление требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства.

   Инструкция: Автоматическая установка обновлений Kaspersky Endpoint Security на 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 Cloud Console 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 Cloud Console и веб-плагинов управления не поддерживается.

   Инструкция: Одобрение и отклонение обновлений программного обеспечения.

По завершении сценария можно перейти к мониторингу состояния сети.

Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"

Чтобы убедиться, что защита ваших управляемых устройств актуальна, вам нужно своевременно обеспечивать обновления следующего:

- Баз и модулей приложений "Лаборатории Касперского".

  Kaspersky Security Center Cloud Console 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 Cloud Console и приложений безопасности.

Эксперты "Лаборатории Касперского" обрабатывают все необходимые обновления для Kaspersky Security Center Cloud Console и его компонентов, а также для управляемых приложений "Лаборатории Касперского". Вы не можете выполнить эти обновления вручную.

В зависимости от конфигурации вашей сети можно использовать следующие схемы загрузки и распространения необходимых обновлений на управляемые устройства:

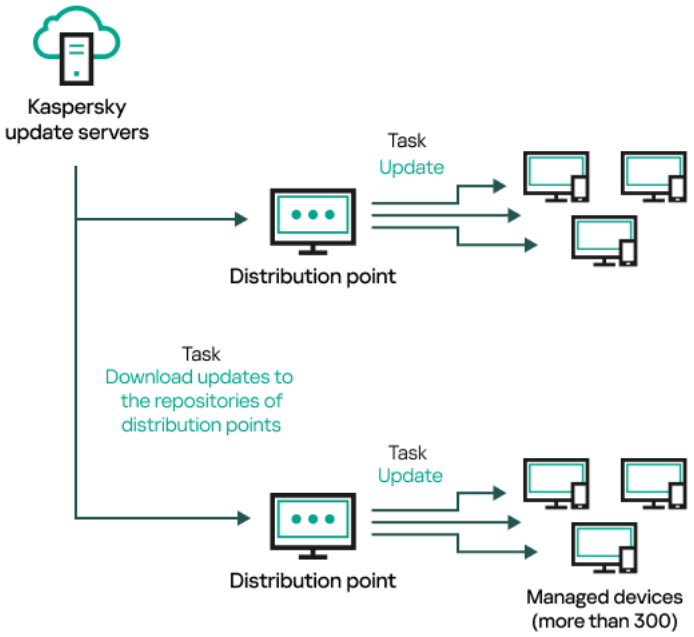
- Использование задачи *Загрузка обновлений в хранилища точек распространения*.
- Вручную через локальную папку, общую папку или FTP-сервер.
- Непосредственно с серверов обновлений "Лаборатории Касперского" для приложений безопасности на управляемых устройствах.

Использование задачи Загрузка обновлений в хранилища точек распространения

В этой схеме Kaspersky Security Center Cloud Console загружает обновления с помощью задачи *Загрузка обновлений в хранилища точек распространения*. Управляемые устройства, входящие в область действия точки распространения, загружают обновления из хранилищ точек распространения (см. рисунок ниже).

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

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



Обновление с использованием задачи Загрузка обновлений в хранилища точек распространения

После завершения задачи *Загрузка обновлений в хранилища точек распространения* следующие обновления загружаются в хранилище точка распространения:

- Базы и модули приложений "Лаборатории Касперского" для приложений безопасности на управляемых устройствах.

  Эти обновления устанавливаются с помощью задачи Обновление Kaspersky Endpoint Security для Windows.

- Обновления для компонентов Kaspersky Security Center Cloud Console.

  По умолчанию эти обновления устанавливаются автоматически. Вы можете изменить параметры политики Агента администрирования.

- Обновления для приложений безопасности.

  По умолчанию приложение Kaspersky Endpoint Security для Windows устанавливает только те обновления, которые вы одобрили. Обновления устанавливаются с помощью задачи Обновление и могут быть настроены в свойствах этой задачи.

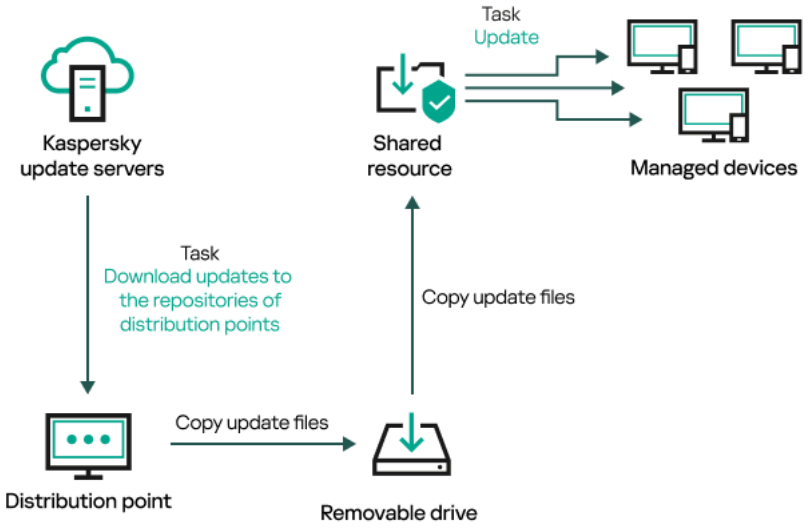
Каждое управляемое приложение "Лаборатории Касперского" запрашивает требуемые обновления с Сервера администрирования. Сервер администрирования объединяет эти запросы и загружает в хранилища точек распространения только те обновления, которые запрашиваются приложениями. Это обеспечивает то, что загружаются только нужные обновления и только один раз. При выполнении задачи *Загрузка обновлений в хранилища точек распространения*, 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.

Передаваемая информация не содержит персональных данных и других конфиденциальных данных. АО "Лаборатория Касперского" защищает полученную информацию в соответствии с установленными законом требованиями.

С помощью локальной папки, общей папки или FTP-сервера

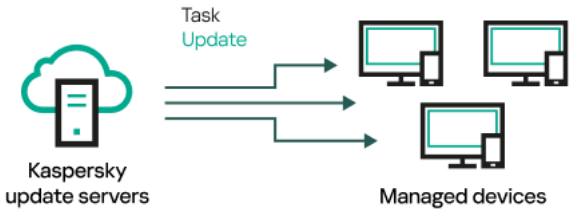
Если клиентские устройства не подключены к точке распространения, можно использовать локальную папку или общий ресурс в качестве источника обновления баз, модулей приложений и приложений "Лаборатории Касперского". В этой схеме вам нужно скопировать необходимые обновления из хранилищ точек распространения на съемный диск, а затем обновления копируются в локальную папку или общий ресурс, указанный в качестве источника обновлений в параметрах Kaspersky Endpoint Security для Windows (см. рисунок ниже).



Обновление через локальную папку, общую папку или FTP-сервер

Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security для Windows на управляемых устройствах

На управляемых устройствах Kaspersky Endpoint Security для Windows получает обновления напрямую с серверов обновлений "Лаборатории Касперского" (см. рисунок ниже).



Обновление приложений безопасности непосредственно с серверов обновлений "Лаборатории Касперского"

В этой схеме приложения безопасности не используют хранилища, предоставленные Kaspersky Security Center Cloud Console. Чтобы получать обновления непосредственно с серверов обновлений "Лаборатории Касперского", укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений в интерфейсе приложения безопасности. Полное описание этих параметров приведено в документации Kaspersky Endpoint Security для Windows.

Создание задачи загрузки обновлений в хранилища точек распространения

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

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

Вы можете создать задачу *Загрузка обновлений в хранилища точек распространения* для группы администрирования. Такая задача будет выполняться для точек распространения, входящих в указанную группу администрирования.

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 Cloud Console;
- 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 **Управление активами → Задачи**.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

3. Для приложения Kaspersky Security Center Cloud Console 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 ("*<>?\:|).

5. Нажмите на кнопку выбора, чтобы указать группу администрирования, выборку устройств или устройства, к которым применяется задача.

6. 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.

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. Сетевая папка может быть FTP-сервером, HTTP-сервером или общим ресурсом SMB. Если сетевая папка требует проверки подлинности, поддерживается только SMB-протокол. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

       > FTP-сервер, HTTP-сервер или сетевая папка, используемые в качестве источника обновлений, должны содержать структуру папок (с обновлениями), которая соответствует структуре папок, созданной при использовании серверов обновлений "Лаборатории Касперского".

   - **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**

  Kaspersky Security Center Cloud Console 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 13.2 или более ранняя версия

  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 13.2 или ниже, 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**

  Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

  - **Вручную** (выбрано по умолчанию)

    Задача не запускается автоматически. Вы можете запустить задачу только вручную.

    По умолчанию выбран этот вариант.

  - **Каждые N минут**

    Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

    По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

  - **Каждый N час**

    Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

    По умолчанию задача запускается каждые 6 часов, начиная с текущих системной даты и времени.

- **Каждые N дней**

  Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются 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 каждый понедельник в текущее системное время.

- **Ежедневно (не поддерживается переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center Cloud Console.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

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

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

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Ежемесячно в 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 выключен.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать 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.

Настройка управляемых устройств для получения обновлений только от точек распространения

Управляемые устройства могут получать обновления баз, модулей приложений и приложения "Лаборатории Касперского" из различных источников: непосредственно с серверов обновлений, от точек распространения, из локальной или сетевой папки. Вы можете указать точки распространения в качестве единственно возможного источника обновлений.

Чтобы настроить получение обновлений управляемыми устройствами только от точек распространения:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на политику Агента администрирования.
3. В окне свойств политики откройте вкладку **Параметры приложения**.
4. В разделе **Параметры** включите переключатель **Распространять файлы только через точки распространения**.

5. Установите замок (🔒) для этого переключателя.

6. Нажмите на кнопку **Сохранить**.

   Политика будет применена к выбранным устройствам и устройства будут получать обновления только от точек распространения.

Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center Cloud Console

Автоматическая установка обновлений для компонентов Kaspersky Security Center Cloud Console включена по умолчанию при установке Агента администрирования на устройство. Вы можете выключить ее при установке Агента администрирования или же выключить позже с помощью политики.

Чтобы выключить автоматическую установку обновлений и патчей для компонентов Kaspersky Security Center Cloud Console при локальной установке Агента администрирования на устройство:

1. Запустите локальную установку Агента администрирования на устройство.

2. На шаге **Дополнительные параметры** снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center со статусом "Не определено"**.

3. Следуйте далее указаниям мастера.

   На устройстве будет установлен Агент администрирования с выключенной автоматической установкой обновлений и патчей для компонентов Kaspersky Security Center Cloud Console. Вы можете включить автоматическую установку позже с помощью политики.

Чтобы выключить автоматическую установку обновлений для компонентов Kaspersky Security Center Cloud Console при установке Агента администрирования на устройство с помощью инсталляционного пакета:

1. В главном окне приложения перейдите в раздел **Операции → Хранилища → Инсталляционные пакеты**.

2. Нажмите на пакет **Агент администрирования Kaspersky Security Center <номер версии>**.

3. В окне свойств выберите вкладку **Параметры**.

4. Выключите переключатель **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**.

   Агент администрирования будет устанавливаться из этого пакета с выключенной автоматической установкой обновлений и патчей для компонентов Kaspersky Security Center Cloud Console. Вы можете включить автоматическую установку позже с помощью политики.

Если при установке Агента администрирования на устройство флажок был установлен (снят) на шаге 4, впоследствии вы можете выключить (включить) автоматическую установку с помощью политики Агента администрирования.

Чтобы включить или выключить автоматическую установку обновлений и патчей для компонентов Kaspersky Security Center Cloud Console с помощью политики Агента администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на политику Агента администрирования.
3. В окне свойств политики выберите раздел **Параметры приложения**.
4. В разделе **Управление патчами и обновлениями** установите включите или выключите переключатель **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"** чтобы включить или выключить автоматическую установку обновлений и патчей.
5. Убедитесь, что установлен (**Принудительно**) замок (🔒) для этого переключателя.

Политика применится к выбранным устройствам, и автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center Cloud Console будет включена (выключена) на этих устройствах.

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 **Управление активами** → **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. 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.
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**. Параметры на этой вкладке определяют, как устройство получает обновления, когда устанавливается соединение между устройством и Сервером администрирования.

    - **Мобильный режим**. Параметры на этой вкладке определяют, как устройство получает обновления, когда не установлено соединение между Kaspersky Security Center Cloud Console и устройством (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.

    Если в качестве источника обновлений установлено приложение Kaspersky Security Center Cloud Console, обновления загружаются из хранилища точки распространения, а не из хранилища Сервера администрирования. Убедитесь, что вы назначили точки распространения и создали задачу *Загрузка обновлений в хранилища точек распространения*.

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 Cloud Console.

    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.

О статусах обновлений

Статус – это атрибут обновлений программного обеспечения, который определяет, должны ли определенные обновления программного обеспечения быть установлены на сетевое устройство.

Обновление может иметь следующие статусы:

- *Не определено.*

  По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Неопределенные обновления могут быть установлены только на Агенте администрирования и других компонентах Kaspersky Security Center Cloud Console в соответствии с параметрами политики Агента администрирования.

- *Одобрено.*

  Одобренные обновления всегда устанавливаются. Если обновление требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения.

- *Отклонено.*

  Обновления, которым вы установили статус *Отклонено*, не устанавливаются на управляемые устройства.

Вы можете изменить статусы обновлений для следующих приложений:

- Агент администрирования и другие компоненты Kaspersky Security Center Cloud Console.

  По умолчанию загруженные обновления и патчи для компонентов Kaspersky Security Center Cloud Console устанавливаются автоматически. Если вы оставили включенным параметр **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"** в свойствах Агента администрирования, тогда все обновления будут установлены автоматически после их загрузки в хранилище (или несколько хранилищ). Если флажок снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрен*.

  Обновления для компонентов Kaspersky Security Center Cloud Console не могут быть удалены, даже если вы установите обновлениям статус *Отклонено*.

- Приложения безопасности "Лаборатории Касперского".

  По умолчанию обновления для управляемых приложений устанавливаются только после изменения статуса обновления на *Одобрено*. Если ранее отклоненное обновление для приложения безопасности было установлено, Kaspersky Security Center Cloud Console попытается удалить обновления со всех устройств.

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 и Linux. Бесшовное обновление Сервера администрирования, Kaspersky Security Center Cloud 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 **Операции** → **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**.

   Чтобы просмотреть данные, обрабатываемые приложениями "Лаборатории Касперского", для которых вы хотите подтвердить бесшовные обновления, нажмите **Просмотреть список данных** в открывшейся панели Лицензионное соглашение.

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 Cloud Console 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.

Использование файлов различий для обновления баз и модулей приложений "Лаборатории Касперского".

Файл различий описывает различия между двумя версиями файлов базы или модулями приложений. Использование файлов различий уменьшает 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 точки распространения, то файлы различий сохраняются на этой точке распространения. В результате устройства, которые получают обновления от этой 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 точки распространения, с которых это устройство получает обновления. Однако трафик может быть сохранен, даже если устройства обновляются в несколько раз реже, чем точка распространения, с которой устройство получает обновления.

Точки распространения не используют многоадресную IP-рассылку для автоматического распространения файлов различий.

Чтобы включить функцию загрузки файлов различий:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Задачи**.
2. Нажмите на имя задачи *Загрузка обновлений в хранилища точек распространения*, чтобы открыть свойства задачи.
3. На вкладке **Параметры приложения** включите параметр **Скачать файлы различий**.
4. Нажмите на кнопку **Сохранить**.

   Функция загрузки файлов различий включена. Файлы различий обновлений загружаются в дополнение к файлам обновлений каждый раз, когда запускается задача *Загрузка обновлений в хранилища точек распространения*.

Чтобы проверить, что функция загрузки файлов различий успешно включена, вы можете измерить внутренний трафик до и после выполнения сценария.

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 хранилищ точек распространения.

Когда вам необходимо обновить базы данных и модули приложений на устройстве (или группе устройств), которое не подключено 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 из следующих источников:

- Точка распространения.

  Чтобы хранилище точки распространения содержало обновления, необходимые для приложения безопасности, установленного на автономном устройстве, по крайней мере на одном из управляемых сетевых устройств должна быть установлено это приложение безопасности. Это приложение должно быть настроено на получение обновлений из хранилища точки распространения с помощью задачи *Загрузка обновлений в хранилища точек распространения*.

- Любое устройство, на котором установлено такое же приложение безопасности и настроено получение обновлений из хранилища точки распространения или напрямую с серверов обновлений "Лаборатории Касперского".

Ниже приведен пример настройки обновлений баз и модулей приложений путем копирования их из хранилища точки распространения.

Чтобы обновить базы данных и модули приложений "Лаборатории Касперского" на автономных устройствах:

1. Подключите съемный диск к устройству, выполняющему роль точки распространения.

2. Скопируйте файлы обновлений на съемный диск.

   По умолчанию обновления хранятся по адресу: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\Updates.

3. На автономных устройствах настройте приложение безопасности (например, Kaspersky Endpoint Security для Windows) на получение обновлений из локальной папки или общего ресурса, такого как FTP-сервер или общая папка.

4. Скопируйте файлы обновлений со съемного диска в локальную папку или общий ресурс, который вы хотите использовать в качестве источника обновлений.

5. На автономном устройстве, на которое требуется установить обновления, запустите задачу обновления Kaspersky Endpoint Security для Windows.

После завершения задачи обновления базы данных и модули приложений "Лаборатории Касперского" будут обновлены на устройстве.

Управление приложениями сторонних производителей на клиентских устройствах

В этом разделе описаны возможности Kaspersky Security Center Cloud Console, связанные с управление сторонних приложений, установленных на клиентских устройствах.

Ограничения Системного администрирования

Возможности Системного администрирования имеют ряд ограничений, которые зависят от режима работы приложения Kaspersky Security Center Cloud Console, используемой по лицензии.

Следующие лицензии не поддерживают Системное администрирование:

- Kaspersky Endpoint Security для бизнеса Стандартный
- Kaspersky Security для виртуальных и облачных сред

Следующие лицензии поддерживают Системное администрирование:

- Kaspersky Endpoint Security для бизнеса Расширенный
- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Total Security для бизнеса
- Kaspersky Security для виртуальных и облачных сред Enterprise

В таблице ниже сравниваются ограничения пробной версии приложения Kaspersky Security Center Cloud Console для лицензий, не поддерживающих Системное администрирования, и для лицензий, поддерживающих Системное администрирование.

Ограничения Системного администрирования

Ограничение	Пробный режим	Коммерческая версия: лицензии, которые не поддерживают Системное администрирование	Коммерческая версия: лицензии, которые поддерживают Системное администрирование
Максимальное количество задач *Установка обновлений Центра обновления Windows* или задач *Закрытие уязвимостей*	4	4	0 (невозможно создавать задачи этих типов)
Максимальное количество задач *Установка требуемых обновлений и закрытие уязвимостей*	2	Не поддерживается	4
Максимальное количество правил во всех задачах *Установка требуемых обновлений и закрытие уязвимостей* на всех серверах, включая виртуальные	10	Не поддерживается	50
Максимальное количество обновлений программного обеспечения, которые могут одновременно иметь статус *Одобрено*, на всех серверах, включая виртуальные	100	Не поддерживается	1000

Максимальное количество обновлений программного обеспечения, которые можно вручную добавить в задачу, на всех серверах, включая виртуальные	500	1000	1000
Максимальное количество уязвимостей в приложениях, которые можно вручную добавить в задачу, на всех серверах, включая виртуальные	500	1000	1000

Доступность Системного администрирования в пробном и коммерческом режимах и при различных вариантах лицензирования

Доступность Системного администрирования в Kaspersky Security Center Cloud Console зависит от того, используете ли вы приложение в пробном или коммерческом режиме, а также от выбранного вами варианта лицензирования. Используйте таблицу, чтобы проверить какие возможности Системного администрирования доступны.

Доступные возможности Системного администрирования

Системное администрирование	Пробный режим	Коммерческая версия: Kaspersky Endpoint Security для бизнеса Стандартный	Коммерческая версия: Kaspersky Endpoint Security для бизнеса Расширенный, Kaspersky Endpoint Detection and Response Optimum, Kaspersky Total Security для бизнеса
Ручное закрытие уязвимостей в приложениях Microsoft на управляемых устройствах под управлением Windows Создание задачи *Закрытие уязвимостей*	✓	✓	–
Ручная установка обновлений программного обеспечения Microsoft на управляемые устройства под управлением Windows Установка обновлений приложений сторонних производителей с помощью задачи *Установка обновлений Центра обновления Windows*	–	✓	✓
Автоматическая установка обновлений приложений сторонних производителей на основе правил и закрытие уязвимостей в приложениях сторонних производителей Создание задачи *Установка требуемых обновлений и закрытие уязвимостей* и установка обновлений Добавление правил для установки обновлений	✓	–	✓

О приложениях сторонних производителей

Kaspersky Security Center Cloud Console может помочь вам обновить приложения сторонних производителей, установленные на клиентских устройствах, и закрыть уязвимости в приложениях сторонних производителей. Kaspersky Security Center Cloud Console 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 Cloud Console, просмотрев список доступных обновлений в Kaspersky Security Center Cloud Console.

Процедура ниже предназначена для просмотра списка стороннего программного обеспечения, которое можно обновить с помощью Kaspersky Security Center Cloud Console. 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 Cloud Console:

1. В главном окне приложения перейдите в раздел **Управление активами** → **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 Cloud Console**.

   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.

Обновления приложений сторонних производителей

Kaspersky Security Center Cloud Console позволяет управлять обновлениями программного обеспечения сторонних производителей, установленных на управляемых устройствах, и закрывать уязвимости в приложениях Microsoft и других производителей программного обеспечения с помощью установки необходимых обновлений.

Kaspersky Security Center Cloud Console 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 устройства.

Обновление некоторых приложений Kaspersky Security Center Cloud Console 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.

Задачи для установки обновлений приложений сторонних производителей

Когда метаданные обновлений приложений сторонних производителей загружаются в хранилище, вы можете установить обновления на клиентские устройства, выполнив следующие задачи:

- Задача *Установка требуемых обновлений и закрытие уязвимостей*.

  Эта задача используется для установки обновлений для приложений Microsoft, включая обновления, предоставляемые службой Центра обновления Windows, и обновления приложений других поставщиков.

  После завершения работы этой задачи обновления устанавливаются на управляемые устройства автоматически. При загрузке метаданных новых обновлений в хранилище Сервера администрирования Kaspersky Security Center Cloud Console проверяет, соответствуют ли обновления критериям, указанным в правилах обновлений. Все новые обновления, которые соответствуют критериям, будут загружены и установлены автоматически при следующем запуске задачи.

- Задача *Установка обновлений Центра обновления Windows*

  Эта задача может использоваться только для установки обновлений Центра обновления Windows.

  После завершения работы этой задачи устанавливаются только те обновления, которые указаны в свойствах задачи. Позже, если вы хотите установить новые обновления, вам нужно добавить требуемые обновления в список обновлений существующей задачи или создать задачу *Установка обновлений Центра обновления Windows*.

Задачи установки обновлений программного обеспечения имеют ряд ограничений. Эти ограничения зависят от типа лицензии, по которой используется приложение Kaspersky Security Center Cloud Console, и от режима работы Kaspersky Security Center Cloud Console.

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 Microsoft и других поставщиков программного обеспечения. Обновления для приложений Microsoft предоставляются службой Центра обновления Windows.

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 Cloud Console 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 мастере первоначальной настройки Kaspersky Security Center Сервера администрирования. Если вы не запустили мастер, создайте задачу или запустите мастер первоначальной настройки.

   Инструкции:

   - Создание задачи Поиск уязвимостей и требуемых обновлений.
   - Параметры задачи поиска уязвимостей и требуемых обновлений.

2. **Анализ списка найденных обновлений**

   Просмотрите список **Обновления ПО** и решите, какие обновления следует установить. Чтобы просмотреть подробную информацию о каждом обновлении, нажмите на имя обновления в списке. Для каждого обновления в списке также можно просмотреть статистику установки обновлений на управляемых устройствах. Например, вы можете просмотреть количество устройств, на которых выбранное обновление не установлено, будет установлено или на которых не удалось установить обновление.

   Инструкции: Просмотр информации о доступных обновлениях приложений сторонних производителей.

3. **Настройка установки обновлений**

После того как Kaspersky Security Center Cloud Console получает список обновлений приложений сторонних производителей, вы можете установить их на клиентские устройства, используя задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Установка обновлений Центра обновления Windows*. Создайте одну из этих задач. Вы можете создать эти задачи на вкладке **Задачи** или с помощью списка **Обновления ПО**.

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.

Задача *Установка обновлений Центра обновления Windows* может использоваться только для установки обновлений Центра обновления Windows.

Задачи установки обновлений программного обеспечения имеют ряд ограничений. Эти ограничения зависят от типа лицензии, по которой используется приложение Kaspersky Security Center Cloud Console, и от режима работы Kaspersky Security Center Cloud Console.

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.

Инструкции:

- Создание задачи Установка требуемых обновлений и закрытие уязвимостей.
- Создание задачи Установка обновлений Центра обновления Windows.
- Просмотр информации о доступных обновлениях приложений сторонних производителей.

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 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 планировании задачи *Установка обновлений Центра обновления Windows* обратите внимание, что для этой задачи вам нужно определять список обновлений каждый раз перед запуском этой задачи.

При задании расписания задач убедитесь, что задача закрытия уязвимостей запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

Инструкции: Общие параметры задач.

5. **Одобрение и отклонение обновлений программного обеспечения (если требуется)**

Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете указать правила установки обновлений в свойствах задачи. Если вы создали задачу *Установка обновлений Центра обновления Windows*, пропустите этот шаг.

Для каждого правила вы можете 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 обновлений Центра обновления Windows и только тех, которые имеют статус *Одобрено*. После этого вы вручную устанавливаете статус *Одобрено* для тех обновлений, которые вы хотите установить. В этом случае обновления Центра обновления Windows со статусом *Не определено* или *Отклонено* не будут установлены на серверы, указанные в задаче.

По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус на *Одобрено* или *Отклонено* в списке **Обновления ПО** (**Операции** → **Управление патчами** → **Обновления ПО**).

Инструкция: Одобрение и отклонение обновлений приложений сторонних производителей.

6. **Запуск задачи установки обновлений**

   Запустите задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Установка обновлений Центра обновления Windows*. После запуска этих задач, обновления загружаются и устанавливаются на управляемые устройства. После завершения задачи убедитесь, что в списке задач она имеет статус *Завершена успешно*.

   Инструкция: Запуск задачи вручную.

7. **Создание отчета о результатах установки обновлений приложений сторонних производителей (если требуется)**

   Чтобы убедиться, что задача создана и обновления установлены, создайте **Отчет о результатах установки обновлений стороннего ПО** и просмотрите подробную статистику установки обновлений в этом отчете.

   Инструкция: Создание и просмотр отчета.

Установка обновлений приложений сторонних производителей

Вы можете установить обновления приложений сторонних производителей на управляемые устройства, создав и запустив одну из следующих задач:

- *Установка требуемых обновлений и закрытие уязвимостей*

  Эту задачу можно использовать для установки обновлений Центра обновления Windows, предоставленных Microsoft, и обновлений приложений других поставщиков.

- *Установка обновлений Центра обновления Windows*

  Эту задачу можно использовать только для установки обновлений Центра обновления Windows.

Задачи установки обновлений программного обеспечения имеют ряд ограничений. Эти ограничения зависят от типа лицензии, по которой используется приложение Kaspersky Security Center Cloud Console, и от режима работы Kaspersky Security Center Cloud Console.

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.

  Доступность мастера установки обновлений зависит от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии.

  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 один из списков обновлений:

   - Чтобы открыть список общих обновлений, в главном меню перейдите в раздел **Операции** → **Управление патчами** → **Обновления ПО**.

   - Чтобы открыть список обновлений для управляемого устройства, в главном меню перейдите в раздел **Управление активами** → **Активы (Устройства)** → **<имя устройства>** → **Дополнительно** → **Применимые обновления**.

   - Чтобы открыть список обновлений для определенного приложения, в главном меню перейдите в раздел **Операции** → **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**.

   Для установки некоторых обновлений программного обеспечения вам нужно принять Лицензионное соглашение. Если вы отклоните Лицензионное соглашение, обновления программного обеспечения не будут установлены.

4. Выберите один из следующих вариантов:

   - **Новая задача**

     Запустится мастер создания задачи. Задача *Установка требуемых обновлений и закрытие уязвимостей* или задача *Установка обновлений Центра обновления Windows* выбрана по умолчанию в зависимости от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии. Следуйте далее указаниям мастера, чтобы завершить создание задачи.

   - **Установить обновление (добавить правило в указанную задачу)**

     Выберите задачу, в которую вы хотите добавить выбранные обновления. Выберите задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Установка обновлений Центра обновления Windows*. Если вы выберите задачу *Установка требуемых обновлений и закрытие уязвимостей*, новое правило для установки выбранных обновлений автоматически добавится в выбранную задачу. Если вы выберете задачу *Установка обновлений Центра обновления Windows*, выбранные обновления будут добавлены в свойства задачи.

     Откроется окно свойств задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы выбрали создание задачи, она создается и отображается в списке задач в разделе **Управление активами** → **Задачи**. Если вы выбрали добавление обновлений в существующую задачу, обновления сохраняются в свойствах задачи.

Чтобы установить обновления приложений сторонних производителей, запустите задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Установка обновлений Центра обновления Windows*. Вы можете запустить эти задачи вручную или задать расписание в свойствах задачи, которую вы запускаете. При указании расписания задачи убедитесь, что задача установки обновления запускается после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

Установка обновлений приложений сторонних производителей с помощью мастера установки обновлений

Доступность этой функции зависит от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии.

Чтобы создать задачу установки обновлений приложений сторонних производителей с помощью мастера установки обновления:

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Обновления 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*
   - *Установка обновлений Центра обновления Windows*
   - *Закрытие уязвимостей*

   Вы не можете изменить задачи двух последних типов для установки новых обновлений. Для установки новых обновлений можно использовать только задачи *Установка требуемых обновлений и закрытие уязвимостей*.

4. Если вы хотите, чтобы мастер отображал только те задачи, которые устанавливают выбранное вами обновление, включите параметр **Показать только задачи, которые устанавливают обновление**.

5. Выберите действие, которое хотите выполнить:

   - Чтобы запустить задачу, установите флажок рядом с именем задачи и нажмите на кнопку **Запустить**.
   - Чтобы добавить новое правило в существующую задачу:

     a. Установите флажок рядом с именем задачи и нажмите на кнопку **Добавить правило**.

     b. На открывшейся странице настройте новое правило:

     - **Правило установки обновлений данного уровня важности**

       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 установки обновлений данного уровня важности по MSRC** (доступно только для обновлений Центра обновления Windows)

  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.

- **Правило установки обновлений данного поставщика** (доступно только для обновлений приложений сторонних производителей)

  Этот параметр доступен только для обновлений приложений сторонних производителей. Kaspersky Security Center Cloud Console 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.

- **Правило установки обновлений типа**

- **Правило установки выбранного обновления**

- **Одобрить выбранные обновления**

  Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

  По умолчанию параметр выключен.

- **Автоматически устанавливать все предыдущие обновления 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**.

- Чтобы создать задачу:

  a. Нажмите на кнопку **Новая задача**.

  b. На открывшейся странице 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.

  - **Правило установки обновлений данного уровня важности по MSRC** (доступно только для обновлений Центра обновления Windows)

    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.

  - **Правило установки обновлений данного поставщика** (доступно только для обновлений приложений сторонних производителей)

    Этот параметр доступен только для обновлений приложений сторонних производителей. Kaspersky Security Center Cloud Console 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.

  - **Правило установки обновлений типа**

  - **Правило установки выбранного обновления**

  - **Одобрить выбранные обновления**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

- **Автоматически устанавливать все предыдущие обновления 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**.

Если вы решили запустить задачу, вы можете закрыть мастер. Задача выполняется в фоновом режиме. Никаких дальнейших действий не требуется.

Если вы выбрали добавление правила к существующей задаче, откроется окно свойств задачи. Новое правило уже добавлено в свойства задачи. Вы можете просмотреть или изменить правило, а также другие параметры задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы решили создать задачу, создайте ее с помощью мастера создания задачи. Новое правило, добавленное вами в мастере установки обновлений, отображается в мастере создания задачи. После завершения работы мастера задача *Установка требуемых обновлений и закрытие уязвимостей* добавлена в список задач.

Создание задачи Поиск уязвимостей и требуемых обновлений

С помощью задачи Поиск уязвимостей и требуемых обновлений Kaspersky Security Center Cloud Console получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, установленных на управляемых устройствах.

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 **Управление активами → Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Security Center Cloud Console 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. 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.
7. Нажмите на кнопку **Создать**.

   Задача будет создана и отобразится в списке задач.
8. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
9. В окне свойств задачи укажите общие параметры задачи.
10. На вкладке **Параметры приложения** укажите следующие параметры:

    - **Поиск уязвимостей и обновлений, перечисленных Microsoft**

      При поиске уязвимостей и обновлений Kaspersky Security Center Cloud Console 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:

      - Сервер администрирования Kaspersky Security Center Cloud Console (см. параметры политики Агента администрирования).
      - Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации.
      - Серверы обновления Microsoft.

      Если этот параметр включен, Агент 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 Cloud Console не запрашивает информацию об обновлениях.

- **Поиск уязвимостей и обновлений сторонних производителей, перечисленных "Лабораторией Касперского"**

  Если этот параметр включен, Kaspersky Security Center Cloud Console 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 Cloud Console 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 Cloud Console 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 пуст.

- **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 Cloud Console. 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 Cloud Console. 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.

11. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

Если результаты задачи содержат предупреждение об ошибке 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", решить эту проблему можно с помощью реестра Windows.

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 Cloud Console 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:

  - Сервер администрирования Kaspersky Security Center Cloud Console (см. параметры политики Агента администрирования).
  - Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации.
  - Серверы обновления Microsoft.

  Если этот параметр включен, Агент 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 Cloud Console не запрашивает информацию об обновлениях.

- **Поиск уязвимостей и обновлений сторонних производителей, перечисленных "Лабораторией Касперского"**

  Если этот параметр включен, Kaspersky Security Center Cloud Console 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 Cloud Console 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 Cloud Console 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 пуст.

- **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 Cloud Console. 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 Cloud Console. 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 Установка требуемых обновлений и закрытие уязвимостей

Доступность задачи *Установка требуемых обновлений и закрытие уязвимостей* зависит от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии.

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.

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*.

Задачи установки обновлений программного обеспечения имеют ряд ограничений. Эти ограничения зависят от типа лицензии, по которой используется приложение Kaspersky Security Center Cloud Console, и от режима работы Kaspersky Security Center Cloud Console.

Чтобы создать задачу Установка требуемых обновлений и закрытие уязвимостей:

1. В главном окне приложения перейдите в раздел **Управление активами → Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Security Center Cloud Console выберите тип задачи **Установка требуемых обновлений и закрытие уязвимостей**.
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 правила для установки обновления, а затем следующие параметры:

   - **Начинать установку в момент перезагрузки или выключения устройства**

     Если флажок установлен, установка обновления выполняется перед перезагрузкой или выключением устройства. В противном случае установка обновлений выполняется по расписанию.

     Установите этот флажок, если установка обновлений может повлиять на производительность устройств.

     По умолчанию параметр выключен.

   - **Устанавливать 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 Cloud Console. 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 Cloud Console. 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.

7. 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.

8. Если вы включите параметр **Завершение создания задачи** на странице **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.

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.

12. Нажмите на кнопку **Сохранить**.

    Задача создана и настроена.

Если результаты задачи содержат предупреждение об ошибке 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", решить эту проблему можно с помощью реестра Windows.

Добавление правил для установки обновлений

Доступность этой функции зависит от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии.

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 обновлений Центра обновления Windows или обновлений 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 необходимо закрыть с помощью установки обновлений.

Вы можете добавить правило для установки обновлений следующими способами:

- Добавить правило при создании задачи Установка требуемых обновлений и закрытие уязвимостей.
- 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.

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 странице **Тип правила** выберите **Правило для всех обновлений**.

3. В окне **Общие критерии** в раскрывающемся списке укажите следующие параметры:

- **Набор обновлений для установки**

  Выберите обновления, которые должны быть установлены на клиентские устройства:

  - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.

  - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.

  - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

- **Закрывать уязвимости с уровнем критичности, равным или выше**

  Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

  Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

  Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

  По умолчанию параметр выключен.

4. В окне **Обновления** выберите обновления для установки:

- **Устанавливать все подходящие обновления**

  В этом случае будут установлены все обновления программного обеспечения, соответствующие критериям, указанным в окне мастера **Общие критерии**. Выбрано по умолчанию.

- **Устанавливать только обновления из списка**

  В этом случае будут установлены обновления только того программного обеспечения, которые вы выбираете вручную в списке. Этот список содержит все доступные обновления программного обеспечения.

  Например, вы можете задать обновления в следующих случаях: чтобы проверить установку обновлений в тестовом окружении, чтобы обновить только критически важные 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.

5. В окне **Уязвимости** выберите уязвимости, которые будут закрыты с установкой указанного обновления:

   - **Закрывать все уязвимости, соответствующие остальным критериям**

     В этом случае будут закрыты все уязвимости программного обеспечения, соответствующие критериям, указанным в окне мастера **Общие критерии**. Выбрано по умолчанию.

   - **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.

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.

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. На странице **Тип правила** выберите **Правило для обновлений Windows Update**.

3. В окне **Общие условия** настройте следующие параметры:

   - **Набор обновлений для установки**

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.

     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.

     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

- **Закрывать уязвимости с уровнем критичности по MSRC, равным или выше**

  Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

  Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный Microsoft Security Response Center (MSRC), равен или превышает значение, выбранное в списке (**Низкий**, **Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

  Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

  По умолчанию параметр выключен.

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.

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 странице **Тип правила** выберите **Правило для сторонних обновлений**.

3. В окне **Общие условия** настройте следующие параметры:

   - **Набор обновлений для установки**

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.
     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

     Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

     По умолчанию параметр выключен.

4. В окне **Приложения** выберите приложения и версии приложений, для которых вы хотите установить обновления. По умолчанию выбраны все приложения.

5. 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.

Создание задачи Установка обновлений Центра обновления Windows

Задача Установка обновлений Центра обновления Windows позволяет устанавливать обновления программного обеспечения, предоставляемые службой Центра обновления Windows, на клиентские устройства.

Задачи установки обновлений программного обеспечения имеют ряд ограничений. Эти ограничения зависят от типа лицензии, по которой используется приложение Kaspersky Security Center Cloud Console, и от режима работы Kaspersky Security Center Cloud Console.

Чтобы создать задачу Установка обновлений Центра обновления Windows:

1. В главном окне приложения перейдите в раздел **Управление активами → Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для приложения Kaspersky Security Center Cloud Console выберите тип задачи **Установка обновлений Центра обновления Windows**.
4. Укажите название задачи, которую вы создаете.

   Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите устройства, которым будет назначена задача.
6. Нажмите на кнопку **Добавить**.

   Откроется список обновлений.
7. Выберите обновления Центра обновлений Windows, которые вы хотите установить и нажмите на кнопку **ОК**.
8. Укажите параметры перезагрузки операционной системы:

   - **Не перезагружать устройство**

     Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

   - **Перезагрузить устройство**

     В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

   - **Запрашивать у пользователя**

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

     По умолчанию выбран этот вариант.

   - **Повторять запрос каждые (мин)**

     Если выбран этот вариант, 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.

9. 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.

10. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

11. Нажмите на кнопку **Готово**.

    Задача будет создана и отобразится в списке задач.

12. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

13. В окне свойств задачи укажите общие параметры задачи в соответствии с вашими требованиями.

14. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

Просмотр информации о доступных обновлениях приложений сторонних производителей.

Вы можете просмотреть список доступных обновлений для приложений сторонних производителей, включая программное обеспечение Microsoft, установленных на клиентских устройствах.

Чтобы просмотреть список доступных обновлений для приложений сторонних производителей, установленных на клиентских устройствах,

В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Обновления ПО**.

Отобразится список доступных обновлений.

Вы можете указать фильтр для просмотра списка обновлений приложений. Нажмите на значок **Фильтр** ( ) в верхнем правом углу списка 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).
     - Категория служб Windows Server Update Services (WSUS), к которой принадлежит обновление.
     - 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. Нажав на статус, откроется список устройств, на которых обновление имеет выбранный статус.

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 → Активы (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 отображаемый список обновлений для приложений сторонних производителей, включая программное обеспечение Microsoft, в файл формата CSV или TXT. Вы можете использовать эти файлы, например, чтобы отправить их вашему начальнику по информационной безопасности или сохранить их в целях статистики.

Чтобы экспортировать список доступных обновлений для приложений сторонних производителей в текстовый файл, установленных на всех управляемых устройствах:

1. В главном окне приложения перейдите в раздел **Операции → Управление патчами → Обновления ПО**.

   На странице отображается список доступных обновлений для приложений сторонних производителей, установленных на всех управляемых устройствах.

2. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать.

Файл, содержащий список доступных обновлений для приложений сторонних производителей, включая программное обеспечение Microsoft, загружается на устройство, которое вы используете в данный момент.

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.

2. Выберите обновления программного обеспечения, которые вы хотите экспортировать.

   Пропустите этот шаг, если вы хотите экспортировать полный список обновлений приложений.

При экспорте полного списка обновлений приложений, будут экспортированы только те обновления, которые отображаются на текущей странице.

Если вы хотите экспортировать только установленные обновления, установите флажок **Показывать установленные обновления**.

3. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать.

Файл, содержащий список обновления приложений сторонних производителей, включая программное обеспечение Microsoft, установленных на выбранных управляемых устройствах, загружается на устройство, которое вы используете в данный момент.

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 статус *Одобрено* целесообразно для небольшого количества обновлений. Чтобы установить несколько обновлений, используйте правила, которые вы можете настроить в задаче *Установка требуемых обновлений и закрытие уязвимостей*. Рекомендуется устанавливать статус *Одобрено* только для тех обновлений, которые не соответствуют критериям, указанным в правилах. При ручном одобрении большого количества обновлений производительность Сервера администрирования снижается, что может привести к перегрузке Сервера администрирования.

Чтобы подтвердить или отменить одно или несколько обновлений:

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Обновления ПО**.

   Отобразится список доступных обновлений.

2. Выберите обновления, которые требуется подтвердить или отклонить.

3. Нажмите на кнопку **Одобрить**, чтобы одобрить выбранное обновление, или **Отклонить**, чтобы отклонить выбранное обновление.

   По умолчанию установлено значение *Не определено*.

Выбранные обновления имеют статусы, которые вы указали.

Также вы можете изменить статус в свойствах требуемого обновления.

Чтобы одобрить или отклонить обновление:

1. В главном окне приложения перейдите в раздел **Операции** → **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, изменив параметр **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. Если вам потребуется удалить их, вы можете сделать это вручную локально.

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*, *Установка обновлений Центра обновления Windows* и *Закрытие уязвимостей*.

Чтобы настроить параметр автоматического обновления для приложения стороннего производителя:

1. В главном окне приложения перейдите в раздел **Операции** → **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 столбцу **Статус автоматических обновлений**.

   Откроется окно свойств приложения.

3. В разделе **Общие** выберите значение для следующего параметра:

   Статус автоматических обновлений

Выберите один из следующих вариантов:

- **Не определено**

  Функция автоматического обновления выключена. Kaspersky Security Center Cloud Console устанавливает обновления приложений сторонних производителей с помощью задач: *Установка требуемых обновлений и закрытие уязвимостей*, *Установка обновлений Центра обновления Windows* 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 Cloud Console устанавливает обновления приложений сторонних производителей с помощью задач: *Установка требуемых обновлений и закрытие уязвимостей*, *Установка обновлений Центра обновления Windows* и *Закрытие уязвимостей*.

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

Настройка автоматического обновления применяется к выбранному приложению.

Обнаружение и закрытие уязвимостей в приложениях

Kaspersky Security Center Cloud Console обнаруживает и закрывает уязвимости в приложениях на управляемых устройствах под управлением операционных систем семейства 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 Cloud Console выполняет поиск известных уязвимостей программного обеспечения на основе признаков из баз данных об известных уязвимостях и базы данных Центра обновления Windows. База данных об известных уязвимостях формируется и поддерживается специалистами "Лаборатории Касперского". Она содержит информацию об уязвимостях, такую как описание уязвимостей, дата обнаружения уязвимостей, уровень критичности уязвимостей. Информация об уязвимостях приложений приведена на сайте "Лаборатории Касперского".

В Kaspersky Security Center Cloud Console для поиска уязвимостей в приложениях используется задача *Поиск уязвимостей и требуемых обновлений*.

Закрытие уязвимостей в приложениях

Для закрытия уязвимостей в приложениях, Kaspersky Security Center Cloud Console использует обновления программного обеспечения выпущенные поставщиками программного обеспечения. Вы можете просмотреть список уязвимостей в приложениях в любое время. Метаданные обновлений программного обеспечения автоматически загружаются в хранилище Сервера администрирования и хранилища точек распространения в результате выполнения задачи *Загрузка обновлений в хранилища точек распространения*. Вы можете создать эту задачу с помощью мастера первоначальной настройки Kaspersky Security Center Cloud Console или вручную.

Обновления программного обеспечения для закрытия уязвимостей могут быть представлены в виде полных дистрибутивов или патчей. Обновления программного обеспечения, которые закрывают уязвимости программного обеспечения, называются *исправлениями*. В Kaspersky Security Center Cloud Console вы закрываете уязвимости, используя *рекомендуемые исправления*. Рекомендуемые исправления это обновления программного обеспечения, которые рекомендуются к установке специалистами "Лаборатории Касперского".

В зависимости от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии вы можете использовать задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Закрытие уязвимостей* для закрытия уязвимостей в приложениях.

Задача *Установка требуемых обновлений и закрытие уязвимостей* автоматически закрывает несколько уязвимостей, устанавливая рекомендуемые исправления. Для этой задачи вы можете вручную настроить определенные правила для закрытия нескольких уязвимостей.

С помощью задачи *Закрытие уязвимостей*, вы можете закрыть уязвимости, установив рекомендуемые исправления для программного обеспечения Microsoft.

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.

Задачи установки обновлений программного обеспечения имеют ряд ограничений. Эти ограничения зависят от типа лицензии, по которой используется приложение Kaspersky Security Center Cloud Console, и от режима работы Kaspersky Security Center Cloud Console.

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 может быть закрыта.

Информация о каждой закрытой уязвимости хранится на Сервере администрирования 90 дней. По истечении этого срока информация удаляется автоматически.

Закрытие уязвимостей в приложениях

После получения списка уязвимостей в приложениях вы можете закрыть уязвимости в приложениях 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*.

Задачи установки обновлений программного обеспечения имеют ряд ограничений. Эти ограничения зависят от типа лицензии, по которой используется приложение Kaspersky Security Center Cloud Console, и от режима работы Kaspersky Security Center Cloud Console.

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.

  Доступность этой функции зависит от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии.

  Мастер упрощает создание и настройку задачи закрытия уязвимостей, а также исключает создание избыточных задач, содержащих те же обновления для установки.

Закрытие уязвимостей в приложениях с помощью списка уязвимостей

Чтобы закрыть уязвимости в приложениях:

1. Откройте один из списков уязвимостей:

   - Чтобы открыть общий список уязвимостей, в главном меню перейдите в раздел **Операции → Управление патчами → Уязвимости в приложениях**.

   - Чтобы открыть список уязвимостей управляемого устройства, в главном меню перейдите в раздел **Управление активами → Активы (Устройства) → имя устройства → Дополнительно → Уязвимости в приложениях**.

   - Чтобы открыть список уязвимостей для требуемого приложения, в главном меню перейдите в раздел **Операции → Сторонние приложения → Реестр приложений → имя приложения → Уязвимости**.

   Отобразится страница со списком уязвимостей в приложениях сторонних производителей.

2. Выберите одну или несколько уязвимостей в списке и нажмите на кнопку **Закрыть уязвимость**.

   Если рекомендуемое обновление программного обеспечения для закрытия одной из выбранных уязвимостей отсутствует, отображается информационное сообщение.

   Для закрытия некоторых уязвимостей программного обеспечения вам нужно принять Лицензионное соглашение для установки программного обеспечения, если это требуется. Если вы отклоняете Лицензионное соглашение, уязвимость в программном обеспечении не закроется.

3. Выберите один из следующих вариантов:

   - **Новая задача**

     Запустится мастер создания задачи. В зависимости от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии, по умолчанию выбрана задача *Установка требуемых обновлений и закрытие уязвимостей* или задача *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. В зависимости от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии выберите задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Закрытие уязвимостей*. В выбранную задачу *Установка требуемых обновлений и закрытие уязвимостей* автоматически добавится новое правило для закрытия выбранных уязвимостей. Если вы выберете задачу *Закрытие уязвимостей*, выбранные уязвимости будут добавлены в свойства задачи.

     Откроется окно свойств задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

   Если вы выбрали создание задачи, она создается и отображается в списке задач в разделе **Управление активами → 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 для закрытия уязвимостей, перечисленных в свойствах задачи.

Закрытие уязвимостей в приложениях с помощью мастера закрытия уязвимостей

Доступность мастера закрытия уязвимостей зависит от действующей лицензии и режима работы Kaspersky Security Center Cloud Console.

Чтобы закрыть уязвимости в приложениях с помощью мастера закрытия уязвимостей:

1. В главном окне приложения перейдите в раздел **Операции → Управление патчами → Уязвимости в приложениях**.

   Откроется страница 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**.

   Откроется мастер закрытия уязвимости. На странице **Выбор задачи закрытия уязвимости** отображается список всех существующих задач следующих типов:

   - *Установка требуемых обновлений и закрытие уязвимостей*
   - *Установка обновлений Центра обновления Windows*
   - *Закрытие уязвимостей*

   Вы не можете изменить последние два типа задач для установки новых обновлений. Для установки новых обновлений можно использовать только задачу *Установка требуемых обновлений и закрытие уязвимостей*.

4. Если вы хотите, чтобы мастер отображал только те задачи, которые закрывают выбранную уязвимость, включите параметр **Показывать только задачи, которые закрывают выбранную уязвимость**.

5. Выберите действие, которое хотите выполнить:

   - Чтобы запустить задачу, установите флажок рядом с именем задачи и нажмите на кнопку **Запустить**.
   - Чтобы добавить новое правило в существующую задачу:

     a. Установите флажок рядом с именем задачи и нажмите на кнопку **Добавить правило**.

     b. На открывшейся странице настройте новое правило:

     - **Правило закрытия уязвимостей данного уровня критичности**

       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** (доступно только для уязвимостей в приложениях Microsoft)

- **Правило закрытия уязвимостей в приложениях выбранного поставщика** (доступно только для уязвимостей в приложениях сторонних производителей)

- **Правило закрытия уязвимости во всех версиях выбранного приложения** (доступно только для уязвимостей в приложениях сторонних производителей)

- **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**.

- 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 закрытия уязвимости с помощью обновлений типа** (доступно только для уязвимостей в приложениях Microsoft)

  - **Правило закрытия уязвимостей в приложениях выбранного поставщика** (доступно только для уязвимостей в приложениях сторонних производителей)

  - **Правило закрытия уязвимости во всех версиях выбранного приложения** (доступно только для уязвимостей в приложениях сторонних производителей)

- **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**.

Если вы решили запустить задачу, вы можете закрыть мастер. Задача выполняется в фоновом режиме. Никаких дальнейших действий не требуется.

Если вы выбрали добавление правила к существующей задаче, откроется окно свойств задачи. Новое правило уже добавлено в свойства задачи. Вы можете просмотреть или изменить правило, а также другие параметры задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы решили создать задачу, создайте ее с помощью мастера создания задачи. Новое правило, добавленное вами в мастер закрытия уязвимостей, отображается в мастере создания задачи. После завершения работы мастера создания задачи, задача *Установка требуемых обновлений и закрытие уязвимостей* добавлена в список задач.

Создание задачи Закрытие уязвимостей

Задача *Закрытие уязвимостей* позволяет закрыть уязвимости в приложениях Microsoft на управляемых устройствах с операционными системами Windows.

Доступность этой функции зависит от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии. 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.

Задачи установки обновлений программного обеспечения имеют ряд ограничений. Эти ограничения зависят от типа лицензии, по которой используется приложение Kaspersky Security Center Cloud Console, и от режима работы Kaspersky Security Center Cloud Console.

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 **Управление активами → Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для приложения Kaspersky Security Center Cloud Console выберите тип задачи **Закрытие уязвимостей**.

4. Укажите название задачи, которую вы создаете.

   Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

5. Выберите устройства, которым будет назначена задача.

6. Нажмите на кнопку **Добавить**.

   Откроется список уязвимостей.

7. Выберите уязвимости, которые вы хотите закрыть и нажмите на кнопку **OK**.

8. Укажите параметры перезагрузки операционной системы:

   - **Не перезагружать устройство**

     Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

   - **Перезагрузить устройство**

     В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

   - **Запрашивать у пользователя**

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

     По умолчанию выбран этот вариант.

   - **Повторять запрос каждые (мин)**

     Если выбран этот вариант, 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.

9. 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.

10. Если вы включите параметр **Завершение создания задачи** на странице **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.

11. Нажмите на кнопку **Готово**.

    Задача будет создана и отобразится в списке задач.

12. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

13. В окне свойств задачи укажите общие параметры задачи в соответствии с вашими требованиями.

14. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

Создание задачи Установка требуемых обновлений и закрытие уязвимостей

Доступность задачи *Установка требуемых обновлений и закрытие уязвимостей* зависит от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии.

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.

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*.

Задачи установки обновлений программного обеспечения имеют ряд ограничений. Эти ограничения зависят от типа лицензии, по которой используется приложение Kaspersky Security Center Cloud Console, и от режима работы Kaspersky Security Center Cloud Console.

Чтобы создать задачу Установка требуемых обновлений и закрытие уязвимостей:

1. В главном окне приложения перейдите в раздел **Управление активами → Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Security Center Cloud Console выберите тип задачи **Установка требуемых обновлений и закрытие уязвимостей**.
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 правила для установки обновления, а затем следующие параметры:

   - **Начинать установку в момент перезагрузки или выключения устройства**

     Если флажок установлен, установка обновления выполняется перед перезагрузкой или выключением устройства. В противном случае установка обновлений выполняется по расписанию.

     Установите этот флажок, если установка обновлений может повлиять на производительность устройств.

     По умолчанию параметр выключен.

   - **Устанавливать 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 Cloud Console. 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 Cloud Console. 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.

7. 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.

8. Если вы включите параметр **Завершение создания задачи** на странице **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.

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.

12. Нажмите на кнопку **Сохранить**.

    Задача создана и настроена.

Если результаты задачи содержат предупреждение об ошибке 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", решить эту проблему можно с помощью реестра Windows.

Добавление правил для установки обновлений

Доступность этой функции зависит от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии.

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 обновлений Центра обновления Windows или обновлений 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 необходимо закрыть с помощью установки обновлений.

Вы можете добавить правило для установки обновлений следующими способами:

- Добавить правило при создании задачи Установка требуемых обновлений и закрытие уязвимостей.
- 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.

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 странице **Тип правила** выберите **Правило для всех обновлений**.

3. В окне **Общие критерии** в раскрывающемся списке укажите следующие параметры:

- **Набор обновлений для установки**

  Выберите обновления, которые должны быть установлены на клиентские устройства:

  - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.

  - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.

  - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

- **Закрывать уязвимости с уровнем критичности, равным или выше**

  Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

  Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

  Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

  По умолчанию параметр выключен.

4. В окне **Обновления** выберите обновления для установки:

- **Устанавливать все подходящие обновления**

  В этом случае будут установлены все обновления программного обеспечения, соответствующие критериям, указанным в окне мастера **Общие критерии**. Выбрано по умолчанию.

- **Устанавливать только обновления из списка**

  В этом случае будут установлены обновления только того программного обеспечения, которые вы выбираете вручную в списке. Этот список содержит все доступные обновления программного обеспечения.

  Например, вы можете задать обновления в следующих случаях: чтобы проверить установку обновлений в тестовом окружении, чтобы обновить только критически важные 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.

5. В окне **Уязвимости** выберите уязвимости, которые будут закрыты с установкой указанного обновления:

   - **Закрывать все уязвимости, соответствующие остальным критериям**

     В этом случае будут закрыты все уязвимости программного обеспечения, соответствующие критериям, указанным в окне мастера **Общие критерии**. Выбрано по умолчанию.

   - **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.

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.

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. На странице **Тип правила** выберите **Правило для обновлений Windows Update**.

3. В окне **Общие условия** настройте следующие параметры:

   - **Набор обновлений для установки**

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.

     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.

     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

- **Закрывать уязвимости с уровнем критичности по MSRC, равным или выше**

  Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

  Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный Microsoft Security Response Center (MSRC), равен или превышает значение, выбранное в списке (**Низкий**, **Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

  Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

  По умолчанию параметр выключен.

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.

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 странице **Тип правила** выберите **Правило для сторонних обновлений**.

3. В окне **Общие условия** настройте следующие параметры:

   - **Набор обновлений для установки**

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.
     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

     Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

     По умолчанию параметр выключен.

4. В окне **Приложения** выберите приложения и версии приложений, для которых вы хотите установить обновления. По умолчанию выбраны все приложения.

5. 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.

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 уязвимостей в приложениях, обнаруженных на всех управляемых устройствах. Если вы запустите задачу для иерархии Серверов администрирования, вы можете просмотреть список управляемых устройств с обнаруженными уязвимостями только для выбранного Сервера администрирования.

Чтобы просмотреть список уязвимостей в приложениях, обнаруженных на всех управляемых устройствах,

В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

На странице отображается список уязвимостей в приложениях, обнаруженных на клиентских устройствах.

Вы также можете сформировать и просмотреть отчет об уязвимостях.

Вы можете указать фильтр для просмотра списка уязвимостей в приложениях. Нажмите на значок **Фильтр** ( ) в верхнем правом углу списка уязвимостей в приложениях для управления фильтром. 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 → Активы (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**.

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 экспортировать список отображаемых уязвимостей в файл формата CSV или TXT. Вы можете использовать эти файлы, например, чтобы отправить их вашему начальнику по информационной безопасности или сохранить их в целях статистики.

Чтобы экспортировать список уязвимостей в приложениях, обнаруженных на всех управляемых устройствах, в текстовый файл:

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. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать.

Файл, содержащий список уязвимостей в приложениях, загружается на устройство, которое вы используете в данный момент.

Чтобы экспортировать список уязвимостей в приложениях, обнаруженных на выбранных управляемых устройствах, в текстовый файл:

1. Откройте список уязвимостей в приложениях, обнаруженных на выбранном управляемом устройстве.

2. Выберите уязвимости в приложениях, которые вы хотите экспортировать.

   Пропустите этот шаг, если вы хотите экспортировать полный список уязвимостей в приложениях, обнаруженных на управляемых устройствах.

   При экспорте полного списка уязвимостей в приложениях, обнаруженных на управляемом устройстве, будут экспортированы только те уязвимости, которые отображаются на текущей странице.

3. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать.

Файл, содержащий список уязвимостей в приложениях, экспортируется с выбранного управляемого устройства, которое вы используете в данный момент.

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**.

   На странице 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 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 → Активы (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.

Сценарий: обнаружение и закрытие уязвимостей в приложениях

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 Cloud Console развернут в вашей организации.
- В сети вашей организации есть управляемые устройства под управлением Windows.

Этапы

Обнаружение и закрытие уязвимостей состоит из следующих этапов:

1. **Поиск уязвимостей в программном обеспечении, установленном на клиентских устройствах**

   Чтобы найти уязвимости в приложениях, установленных на управляемых устройствах, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Kaspersky Security Center Cloud Console 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 мастере первоначальной настройки Kaspersky Security Center Cloud Console. Если вы не запускали мастер первоначальной настройки, запустите его сейчас или создайте задачу вручную.

   Инструкции: Создание задачи Поиск уязвимостей и требуемых обновлений.

2. **Анализ списка обнаруженных уязвимостей в приложениях**

   Просмотрите список **Уязвимости в приложениях** и решите, какие уязвимости требуется закрыть. Чтобы просмотреть подробную информацию о каждой уязвимости, нажмите на имя уязвимости в списке. Для каждой уязвимости в списке вы также можете просмотреть статистику уязвимости на управляемых устройствах.

   Инструкции:

   - Просмотр информации об уязвимостях в приложениях.
   - Просмотр статистики уязвимостей на управляемых устройствах.

3. **Настройка закрытия уязвимостей**

   Обнаружив уязвимости в приложениях, вы можете закрыть уязвимости в приложениях на управляемых устройствах, используя задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *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. Доступность этой задачи зависит от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии. Чтобы устранить уязвимости в приложениях, задача *Установка требуемых обновлений и закрытие уязвимостей* использует рекомендованные обновления приложений.

Задача *Закрытие уязвимостей* использует рекомендуемые исправления для программного обеспечения Microsoft.

Вы можете запустить мастер закрытия уязвимостей, который автоматически создаст одну из этих задач, или вы можете создать одну из этих задач вручную.

Инструкция: Закрытие уязвимостей в приложениях сторонних производителей, Создание задачи Установка требуемых обновлений и закрытие уязвимостей.

4. **Задание расписания задачи**

   Чтобы убедится, что список уязвимостей всегда актуален, задайте расписание запуска задачи *Поиск уязвимостей и требуемых обновлений*, чтобы она периодически запускалась автоматически. Рекомендуемый средний период – один раз в неделю.

   Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете задать ее запуск с той же периодичностью, что и для задачи *Поиск уязвимостей и требуемых обновлений*, или реже. При задании расписания задачи *Закрытие уязвимостей*, вам нужно выбрать исправления приложений Microsoft 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 уязвимости в приложениях, которые должны быть закрыты на всех управляемых устройствах или только на выбранных управляемых устройствах.

   Инструкция: Игнорирование уязвимостей в приложениях

6. **Запуск задачи закрытия уязвимости**

   Запустите задачу *Установка требуемых обновлений и закрытие уязвимостей* или *Закрытие уязвимостей*. После завершения задачи 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 отчете отображается информация об уязвимостях в приложениях, которые не закрыты. Таким образом, вы можете иметь представление об обнаружении и закрытии уязвимостей в приложениях сторонних производителей в вашей организации, включая программное обеспечение Microsoft.

   Инструкция: Создание и просмотр отчета.

8. **Проверка настройки обнаружения и закрытия уязвимостей в приложениях сторонних производителей**

   Убедитесь в следующем:

   - Список уязвимостей в приложениях на управляемых устройствах не пустой.
   - В списке задач есть задача закрытия уязвимостей.

- Запуск задач для поиска и закрытия уязвимостей в приложениях настроен так, чтобы они запускались последовательно. Просмотрите свойства этих задач и сравните их расписание.

- Задача закрытия уязвимостей в приложениях успешно выполнена. Просмотрите информацию в окне свойств задачи на вкладке **Результаты**.

Результаты

Если вы создали и настроили задачу *Установка требуемых обновлений и закрытие уязвимостей*, уязвимости будут автоматически закрыты на управляемых устройствах. При запуске задачи, задача выполняет сопоставление списка доступных обновлений программного обеспечения с правилами, указанными в параметрах задачи. Все обновления программного обеспечения, которые соответствуют критериям правил, будут загружены в хранилище точки распространения и будут установлены для закрытия уязвимостей в приложениях, кроме обновлений Центра обновления Windows. Для установки обновлений Windows вам необходимо обеспечить доступ к общедоступным серверам Центра обновления Windows на ваших управляемых устройствах.

Если вы создали задачу *Закрытие уязвимостей*, закрываются только уязвимости в приложениях Microsoft.

Установка максимального срока хранения информации о закрытых уязвимостях

Чтобы установить максимальный срок хранения в базе данных информации об уже закрытых уязвимостях на управляемых устройствах:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На открывшейся странице перейдите на вкладку **Хранилище событий**.

3. Укажите максимальный срок хранения информации о закрытых уязвимостях в базе данных.

   По умолчанию срок хранения составляет 7 дней в пробном режиме и 60 дней в коммерческом режиме. Максимальный срок хранения – 14 дней в пробном режиме и 365 дней в коммерческом режиме.

4. Нажмите на кнопку **Сохранить**.

Максимальный срок хранения информации о закрытых уязвимостях ограничен указанным количеством дней.

Управление запуском приложений на клиентских устройствах

В этом разделе описаны возможности Kaspersky Security Center Cloud Console связанные с управлением приложений, запущенных 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 Cloud Console развернут в вашей организации.
- Политика Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux создана и активна.

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.

   Инструкция: Получение и просмотр списка исполняемых файлов, установленных 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.

   Инструкция: Создание пополняемой вручную категории приложений, Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств

3. **Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows**

   Настройте компонент Контроль приложений в политике Kaspersky Endpoint Security для Windows 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: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows. Следуйте этой инструкции и включите тестовый режим в процессе настройки.

5. **Изменение параметров категорий компонента Контроль приложений**

   Если требуется, измените параметры компонента Контроль приложений. На основании результатов тестирования вы можете добавить исполняемые файлы, связанные с событиями компонента Контроль приложений, в категорию приложений пополняемую вручную.

   Инструкция: Добавление исполняемых файлов, связанных с событием, в категорию приложения.

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: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows. Следуйте этой инструкции и выключите тестовый режим в процессе настройки.

7. **Проверка конфигурации Контроля приложений**

   Убедитесь в следующем:

   - Список категорий для исполняемых файлов не пуст. Просмотрите список категорий и убедитесь, что он содержит настроенные вами категории приложений.
   - Контроль приложений настроен на использование созданных категорий приложений. Просмотрите параметры политики Kaspersky Endpoint Security для Windows и убедитесь, что вы настроили Контроль приложений на вкладке **Параметры приложения** → **Контроль безопасности** → **Контроль приложений**.
   - Правила Контроля приложений применены в рабочем режиме. Проверьте режим в политике Kaspersky Endpoint Security для Windows и убедитесь, что вы выключили **Тестовый режим** на вкладке **Параметры приложения** → **Контроль безопасности** → **Контроль приложений**.

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.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux

Режимы и категории компонента Контроль приложений

Компонент Контроль приложений контролирует попытки пользователей запуска приложений. Вы можете использовать правила компонента Контроль приложений для контроля запуска приложений.

Компонент Контроль приложений доступен для приложений Kaspersky Endpoint Security для Windows и Kaspersky Endpoint Security для Linux (версии 11.2 и выше). Все инструкции в этом разделе описывают настройку Контроля приложений для приложения Kaspersky Endpoint Security.

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 режим *Список запрещенных*.
- *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 Cloud Console существует два типа категорий:

- Пополняемая вручную категория. Вы определяете условия, например, метаданные файла, хеш файла, сертификат файла, KL-категория, путь к файлу, чтобы включить исполняемые файлы в категорию.
- Категория, в которую входят исполняемые файлы с выбранных устройств. Вы указываете устройство, исполняемые файлы которого автоматически включаются в категорию.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux

Получение и просмотр списка приложений, установленных на клиентских устройствах

Kaspersky Security Center Cloud Console выполняет инвентаризацию программного обеспечения, которое установлено на управляемых клиентских устройствах, работающих под управлением операционной системы Linux и Windows.

Агент администрирования составляет список приложений, установленных на устройстве, и передает список Серверу администрирования. Агенту администрирования требуется около 10–15 минут для обновления списка приложений.

Для клиентских устройств с операционной системой Windows Агент администрирования получает большую часть информации об установленных приложениях из реестра Windows. Для клиентских устройств с операционной системой Linux информацию об установленных приложениях Агент администрирования получает от диспетчеров пакетов.

Чтобы просмотреть список приложений, установленных на управляемых устройствах,

1. В главном окне приложения перейдите в раздел **Операции** → **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, список доступных обновлений программного обеспечения или список обнаруженных уязвимостей программного обеспечения.

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 таблицы** 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** → **Активы (Устройства)** → **<имя устройства>** → **Дополнительно** → **Реестр приложений**. В этом меню можно экспортировать список приложений в файлы форматов CSV или TXT.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux

Получение и просмотр списка исполняемых файлов, установленных 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 следующих приложений:

- Kaspersky Endpoint Security для Windows.
- Kaspersky Endpoint Security для Linux (версии 11.2 и выше).

Вы можете снизить нагрузку на базу данных при получении информации об установленных приложениях. Для этого рекомендуется запускать 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 **Управление активами** → **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 Windows или Kaspersky Endpoint Security для Linux в зависимости от типа операционной системы клиентских устройств.
4. В раскрывающемся списке **Тип задачи** выберите **Инвентаризация**.
5. На странице **Завершение создания задачи** нажмите на кнопку **Готово**.

После того как мастер создания задачи завершит свою работу, задача **Инвентаризация** будет создана и настроена. Вы можете изменить параметры созданной задачи. В результате созданная задача отобразится в списке задач.

Подробное описание задачи инвентаризации см. в следующих справках:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux

После выполнения задачи **Инвентаризация** формируется список исполняемых файлов, установленных 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 **Операции** → **Сторонние приложения** → **Исполняемые файлы**.

На странице отобразится список исполняемых файлов, установленных на клиентских устройствах.

При необходимости вы можете отправить исполняемый файл управляемого устройства на устройство, где открыто приложение Kaspersky Security Center Cloud Console.

Чтобы отправить исполняемый файл:

1. В главном окне приложения перейдите в раздел **Операции** → **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. Для этого вы можете использовать точку распространения в качестве push-сервера с портом по умолчанию (13295) или установить флажок **Не разрывать соединение с Сервером администрирования**. Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

4. Нажмите на кнопку **Отправить**.

Выбранный исполняемый файл будет загружен для дальнейшей отправки на устройство, на котором открыто приложение Kaspersky Security Center Cloud 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 **Операции** → **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** 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 списка:

   - **Из KL-категории**

     Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать категорию приложений "Лаборатории Касперского". Приложения, входящие в указанную KL-категорию, будут добавлены в пользовательскую категорию приложений.

   - **Выберите сертификат из хранилища сертификатов**

     Если выбран этот вариант, можно указать сертификаты из хранилища. 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 файл или папку на клиентском устройстве, исполняемые файлы из которой будут добавлены в пользовательскую категорию приложений. Вы можете использовать регулярные выражения, такие как *C:\path_to_exe**, например: *C:\Program Files\Internet Explorer**.

- **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 Cloud Console 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 10 Service Pack 2 для Windows и выше поддерживают вычисление хеш-функции SHA256. Вычисление хеш-функции MD5 поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows.

Выберите один из вариантов вычисления хеш-функции приложением Kaspersky Security Center Cloud Console для файлов категории:

- Если все экземпляры приложений безопасности, установленных в вашей сети, являются версиями приложения Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, установите флажок **SHA256**. Не рекомендуется добавлять категорию, созданную по критерию SHA256 исполняемого файла, для версий приложений ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows. Это может привести к сбою приложения безопасности. В этом случае вы можете использовать криптографическую хеш-функцию MD5 для файлов категории.

- Если в вашей сети установлены более ранние версии, чем Kaspersky Endpoint Security 10 Service Pack 2 для Windows, выберите **MD5-хеш**. Добавить категорию, созданную по критерию контрольной суммы MD5 исполняемого файла, для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, невозможно. В этом случае вы можете использовать криптографическую хеш-функцию SHA256 для файлов категории.

- Если разные устройства в вашей сети используют как более ранние, так и более поздние версии Kaspersky Endpoint Security 10, установите флажок **SHA256** и флажок **MD5-хеш**.

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 файла MSI-пакета/архивной папки**

  Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать файл установщика MSI. Метаданные установщика приложения будут передаваться на Сервер администрирования. Приложения, у которых метаданные установщика совпадают с указанным установщиком MSI, будут добавлены в пользовательскую категорию приложений.

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 столько критериев для создания категории приложений, сколько вам нужно.

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 мастера создается категория приложений. Оно появится в списке категорий приложений. Вы можете создать категорию приложений при настройке компонента Контроль приложений.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux

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 и использовать ее для настройки компонента Контроль приложений.

Чтобы создать категорию, в которую входят исполняемые файлы с выбранных устройств:

1. В главном окне приложения перейдите в раздел **Операции** → **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.

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 Cloud Console 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 10 Service Pack 2 для Windows и выше поддерживают вычисление хеш-функции SHA256. Вычисление хеш-функции MD5 поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows.

Выберите один из вариантов вычисления хеш-функции приложением Kaspersky Security Center Cloud Console для файлов категории:

- Если все экземпляры приложений безопасности, установленных в вашей сети, являются версиями приложения Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, установите флажок **SHA256**. Не рекомендуется добавлять категорию, созданную по критерию SHA256 исполняемого файла, для версий приложений ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows. Это может привести к сбою приложения безопасности. В этом случае вы можете использовать криптографическую хеш-функцию MD5 для файлов категории.

- Если в вашей сети установлены более ранние версии, чем Kaspersky Endpoint Security 10 Service Pack 2 для Windows, выберите **MD5-хеш**. Добавить категорию, созданную по критерию контрольной суммы MD5 исполняемого файла, для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, невозможно. В этом случае вы можете использовать криптографическую хеш-функцию SHA256 для файлов категории.

Если разные устройства в вашей сети используют как более ранние, так и более поздние версии Kaspersky Endpoint Security 10, установите флажок **SHA256** и флажок **MD5-хеш**.

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.

Просмотр списка категорий приложений

Вы можете просмотреть список настроенных категорий приложений и параметры каждой категории приложений.

Чтобы просмотреть список категорий приложений,

В главном окне приложения перейдите в раздел **Операции** → **Сторонние приложения** → **Категории приложений**.

Откроется страница со списком категорий приложений.

Чтобы просмотреть свойства категории приложений,

нажмите на имя категории приложений.

Откроется окно свойств выбранной категории приложений. Параметры сгруппированы на нескольких вкладках.

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 Программ [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 **ОК**.

    Окно **Категории приложений** закрывается.

14. В окне правил **Контроль приложений** в разделе **Субъекты и их права** создайте список пользователей и групп пользователей, чтобы применить к ним правила Контроля приложений.

15. Нажмите на кнопку **ОК**, чтобы сохранить параметры и закрыть окно **Правило Контроля приложений**.

16. Нажмите на кнопку **ОК**, чтобы сохранить параметры и закрыть окно **Списки запрещенных и разрешенных**.

17. Нажмите на кнопку **ОК**, чтобы сохранить параметры и закрыть окно **Контроль приложений**.

18. Закройте окно с параметрами политики Kaspersky Endpoint Security для Windows.

Компонент Контроль приложений настроен. После распространения политики на клиентские устройства запуск исполняемых файлов контролируется.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux

Добавление исполняемых файлов, связанных с событием, в категорию приложения

После настройки компонента Компонента Контроль приложений в политиках Kaspersky Endpoint Security для Windows 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 MD5 (для совместимости с Kaspersky Endpoint Security 10 Service Pack 1)**

  Каждый файл имеет свою уникальную хеш-функцию MD5. При выборе хеш-функции MD5 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

  Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции MD5 исполняемого файла. Вычисление хеш-функции MD5 поддерживается для версий Kaspersky Endpoint Security 10 Service Pack 1 для Windows и ниже.

5. Нажмите на кнопку **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.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux

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".

Создание инсталляционных пакетов приложений сторонних производителя из базы "Лаборатории Касперского" доступно только при наличии лицензии на Системное администрирование.

Чтобы создать инсталляционный пакет для приложения стороннего производителя из базы "Лаборатории Касперского":

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.

2. Нажмите на кнопку **Добавить**.

3. На открывшейся странице мастера создания инсталляционного пакета выберите параметр **Выбрать приложение из базы "Лаборатории Касперского" для создания инсталляционного пакета** и нажмите на кнопку **Далее**.

4. В открывшемся списке приложений выберите соответствующее приложение и нажмите на кнопку **Далее**.

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 открывшейся странице **Лицензионное соглашение** перейдите по ссылке на веб-сайте производителя, чтобы прочитать Лицензионное соглашение, а затем установите флажок **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения настоящего Лицензионного соглашения**.

7. На открывшейся странице **Имя нового инсталляционного пакета** в поле **Имя пакета** укажите имя инсталляционного пакета и нажмите на кнопку **Далее**.

Дождитесь загрузки созданного инсталляционного пакета на Сервер администрирования. После того как мастер создания инсталляционного пакета отобразит сообщение, информирующее вас, что процесс создания пакета успешно завершен, нажмите на кнопку **Готово**.

Созданный инсталляционный пакет появится в списке инсталляционных пакетов. Вы можете выбрать этот пакет при создании или перенастройке задачи *Удаленная установка приложения*.

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 **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.

2. В открывшемся списке инсталляционных пакетов нажмите на имя соответствующего пакета.

3. На открывшейся странице свойств измените параметры, если это требуется.

4. Нажмите на кнопку **Сохранить**.

Изменения сохранены.

Параметры инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"

Параметры инсталляционного пакета приложения стороннего производителя сгруппированы на следующих вкладках:

По умолчанию отображается только часть параметров, перечисленных ниже. Вы можете добавить соответствующие графы, нажав на кнопку **Фильтр** и выбрав соответствующие графы 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.

- **Отозвано**

  Отображается дата и время, когда обновление было отозвано.

- **Статус одобрения обновления**

  Отображается, одобрена ли установка обновления.

- **Ревизия**

  Отображается номер текущей ревизии обновления.

- **Идентификатор обновления**

  Отображается идентификатор обновления.

- **Версия 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.

- 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 ревизии инсталляционного пакета.

  - **Время** – дата и время изменения параметров инсталляционного пакета.

  - **Пользователь** – имя пользователя, изменившего параметры инсталляционного пакета.

  - **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.

Теги приложений

Kaspersky Security Center Cloud Console 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 **Операции** → **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 переименовать тег приложения:

1. В главном окне приложения перейдите в раздел **Операции** → **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 имя тега.
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 **Операции** → **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 **Операции** → **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 **Операции** → **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.

Настройка Сервера администрирования

В этом разделе описан процесс настройки и свойства Сервера администрирования.

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. Для Сервера администрирования, который находится в инфраструктуре "Лаборатории Касперского", и главный, и подчиненный Серверы администрирования в вашей сети являются подчиненными. Вы можете добавить как Сервер администрирования с системой Windows, так и Сервер администрирования с 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.

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 Cloud Console, 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

Вы можете назначить Сервер администрирования, работающий локально, подчиненным Сервером, установив таким образом отношение иерархии "главный Сервер – подчиненный Сервер" внутри вашей сети. Для Сервера администрирования, который находится в инфраструктуре "Лаборатории Касперского", и главный, и подчиненный Серверы администрирования в вашей сети являются подчиненными. Вы можете добавить как Сервер администрирования с системой Windows, так и Сервер администрирования с системой Linux.

Чтобы добавить подчиненный Сервер администрирования, доступный для подключения:

1. Убедитесь, что на будущем подчиненном Сервере администрирования установлено приложение Kaspersky Security Center Web Console.

2. На будущем подчиненном Сервер администрирования загрузите сертификат Сервера администрирования и сохраните его, чтобы его можно было добавить на главный Сервер администрирования на одном из шагов мастера добавления подчиненного Сервера администрирования.

3. Выполните следующие действия через Kaspersky Security Center Web Console на будущем подчиненном Сервере администрирования (также вы можете предложить выполнить эти действия администратору будущего подчиненного Сервера администрирования):

   a. Перейдите в свойства будущего главного Сервера администрирования, нажав на название Сервера администрирования в главном меню.

      Вы также можете перейти к свойствам нужного Сервера администрирования из панели навигации. Для этого в главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Settings**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**. В открывшейся панели наведите курсор мыши на название нужного Сервера администрирования и нажмите на значок параметров (⚙).

   b. В открывшемся окне свойств перейдите в раздел **Иерархия Серверов администрирования** на вкладку **Общие**.

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

   d. Выберите тип **Cloud Console** в качестве типа главного Сервера администрирования.

      Поля становятся доступными для установки соединения между подчиненным и главным Серверами администрирования.

   e. В полях **Адрес HDS-сервера (для главного Сервера администрирования на Kaspersky Security Center Cloud Console)** и **Порты HDS-сервера** укажите адрес и порт главного Сервера администрирования Kaspersky Security Center Cloud Console.

      Вы можете найти адрес HDS-сервера и порт HDS-сервера в интерфейсе Kaspersky Security Center Cloud Console Administration Server в разделе **Иерархия Серверов администрирования** на вкладке **Общие** окна свойств. Вы можете скопировать и вставить эти данные в поля окна свойств подчиненного Сервера администрирования.

f. Нажмите на кнопку **Укажите сертификат главного Сервера администрирования** и выберите сертификат.

Вы можете загрузить этот сертификат с Сервера администрирования Kaspersky Security Center Cloud Console в разделе **Иерархия Серверов администрирования** на вкладке **Общие** окна свойств, нажав на кнопку **Посмотреть сертификат Сервера**.

g. Нажмите на кнопку **Укажите сертификат службы Hosted Discovery Service** и выберите сертификат.

Вы можете загрузить этот сертификат с Сервера администрирования Kaspersky Security Center Cloud Console в разделе **Иерархия Серверов администрирования** на вкладке **Общие** в окне свойств, нажав на кнопку **HDS-сертификат, выпущенный корневым центром сертификации**.

h. Если вы используете прокси-сервер для подключения к Серверу администрирования Kaspersky Security Center Cloud Console (то есть к главному Серверу в построенной вами иерархии), укажите это и введите учетные данные прокси-сервера.

i. Выберите параметр **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**, если подчиненный Сервер администрирования находится в демилитаризованной зоне (DMZ).

j. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения и закрыть окно.

4. В главном меню Kaspersky Security Center Cloud Console нажмите на имя Сервера администрирования.

5. На открывшейся странице свойств нажмите на вкладку **Серверы администрирования**.

6. Установите флажок рядом с именем группы администрирования, в которую вы хотите добавить подчиненный Сервер администрирования.

7. В меню выберите пункт **Подключить подчиненный Сервер администрирования**.

Запустится мастер добавления подчиненного Сервера администрирования. Для продолжения работы мастера нажмите на кнопку **Далее**.

8. Заполните следующие поля:

- **Имя подчиненного Сервера администрирования**

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

- **Адрес подчиненного Сервера администрирования (необязательно)**

  Укажите IP-адрес или доменное имя подчиненного Сервера администрирования.

  Этот параметр необходим, если включен параметр **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.

9. Если вы используете прокси-сервер для подключения к Серверу администрирования Kaspersky Security Center Cloud Console (то есть будущему главному Серверу), укажите это и введите учетные данные прокси-сервера.

10. Следуйте далее указаниям мастера.

После завершения работы мастера иерархия "главный Сервер – подчиненный Сервер" создана. Главный Сервер начинает принимать подключение от подчиненного Сервера 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.

Настройка срока хранения событий, относящихся к удаленным устройствам

В Kaspersky Security Center Cloud Console события хранятся в хранилище событий. Вы не можете настраивать количество событий, которые хранятся в хранилище событий.

В окне свойств Сервера администрирования, в разделе **Хранилище событий** вы можете настроить максимальный срок хранения событий, относящихся к удаленным устройствам. Максимальный срок хранения – 1000 дней.

Чтобы настроить количество дней хранения событий, относящихся к удаленным устройствам:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Хранилище событий**.

3. Включите параметр **Хранить события после удаления устройств**.

4. В блоке **Максимальное время хранения (сут)** укажите количество дней хранения событий, относящихся к удаленным устройствам.

Количество дней хранения событий, относящихся к удаленным устройствам, ограничено указанным значением.

Также можно изменить параметры любой задачи, чтобы сохранять события, связанные с ходом выполнения задачи, или сохранять только результаты выполнения задачи. Таким образом вы уменьшаете количество событий в базе данных, увеличиваете скорость работы сценариев, связанных с анализом таблицы событий в базе данных, и снижаете риск вытеснения критических событий большим количеством событий.

Объединение электронной почты о событиях

Во время работы Kaspersky Security Center Cloud Console и управляемые приложения "Лаборатории Касперского" генерируют события. 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 Kaspersky Security Center Cloud Console может присваивать событиям одного типа разные уровни важности.

Kaspersky Security Center Cloud Console автоматически отправляет уведомления о событиях по электронной почте. Kaspersky Security Center Cloud Console отправляет уведомления о событиях, перечисленных в окне **Свойства Сервера администрирования** на вкладке **Настройка событий**. Общие параметры уведомлений используются для всех типов событий.

Чтобы ограничить количество отправляемых электронных писем, Kaspersky Security Center Cloud Console объединяет события с одинаковым уровнем важности за указанные периоды. Значения периодов управляются специалистами "Лаборатории Касперского". При необходимости вы можете просмотреть информацию об интервалах объединения, **перейдя по этой ссылке**.

После отправки уведомления о новом событии с определенным уровнем важности Сервер администрирования выполняет следующие действия:

1. Активирует пятнадцатиминутный счетчик.

2. Через 15 минут:

   - Если не произошло ни одного события такого же или более низкого уровня важности, счетчик сбрасывается.

   - Если происходит хотя бы одно событие с таким же или более низким уровнем важности, отправляет получателям одно объединенное письмо с информацией о событиях, а затем активирует другой счетчик с трехчасовым интервалом.

     В этом случае Сервер администрирования выполняет одно из следующих действий:

     - Если в течение этих трех часов не произошло ни одного события соответствующего (или более низкого) уровня важности, оба счетчика сбрасываются.

     - Если происходит хотя бы одно событие с таким же или более низким уровнем важности, отправляет получателям одно объединенное электронное письмо с информацией о событиях и повторно активирует трехчасовой счетчик.

Если в течение одного из интервалов (15 минут или 3 часов) происходит хотя бы одно событие с более высоким уровнем важности, Сервер администрирования последовательно выполняет следующие действия:

a. Отправляет получателям одно объединенное письмо с информацией о ранее накопленных событиях, не дожидаясь окончания интервала.

b. Отправляет получателям электронное сообщение о новом событии с более высоким уровнем важности.

c. Сбрасывает активные счетчики.

d. Активирует новый 15-минутный счетчик и описанный здесь сценарий будет перезапущен.

В результате получателям приходят объединенные электронные письма в соответствии со следующим шаблоном: "Произошли события: <Количество> <Уровень_важности> (и более низкого уровня)".

Если вы хотите получать уведомления от пользователей немедленно, вы можете настроить интеграцию между Kaspersky Security Center Cloud Console и SIEM, а затем настроить уведомления о необходимых событиях из SIEM.

Ограничения на управление подчиненными Серверами администрирования, работающими локально, с помощью Kaspersky Security Center Cloud Console

После перехода на подчиненный Сервер администрирования, работающий локально, с помощью соответствующего параметра в Kaspersky Security Center Cloud Console, приложение накладывает определенные ограничения на управление этим подчиненным Сервером администрирования. Следующие параметры, относящиеся к работе Kaspersky Security Center Cloud Console, становятся недоступными для пользователя:

- В свойствах политик Агента администрирования и политик Сервера администрирования вкладки **Настройка событий** и **Параметры приложения** недоступны; невозможно создать политики.
- В свойствах задач Агента администрирования и задач Сервера администрирования вкладки **Настройка событий** и **Параметры приложения** недоступны; невозможно создать задачи.
- Управление Агентом администрирования и Сервером администрирования недоступно, также недоступно окно свойств подчиненного Сервера администрирования.
- Мастер первоначальной настройки недоступен.
- Параметры хранения событий и уведомлений для Агента администрирования и Сервера администрирования не могут быть изменены.
- Раздел **Текущие версии приложений** недоступен.
- Раздел **Инсталляционные пакеты** недоступен.

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: **Активы (Устройства)**, **Политики**, **Задачи** и **Точки распространения**. Иначе группы отображаются серым цветом.

Удаление иерархии Серверов администрирования

Если вам больше не нужна иерархия Серверов администрирования, вы можете отключить их от этой иерархии.

Чтобы удалить иерархию Серверов администрирования:

1. В главном меню нажмите на имя главного Сервера администрирования.
2. На открывшейся странице перейдите на вкладку **Серверы администрирования**.
3. В группе администрирования, в которой вы хотите удалить подчиненный Сервер администрирования, выберите подчиненный Сервер администрирования.
4. В меню выберите пункт **Удалить**.
5. В открывшемся окне нажмите на кнопку **ОК** для подтверждения удаления подчиненного Сервера администрирования.

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

Настройка интерфейса

Вы можете настроить интерфейс Kaspersky Security Center Cloud Console, чтобы отобразить или скрыть разделы и элементы интерфейса в зависимости от используемых функций.

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

1. В главном окне приложения перейдите в раздел **Параметры** → **Параметры интерфейса**.
2. В появившемся окне **Параметры интерфейса** включите или выключите параметры:
   - **Показать раздел "Шифрование и защита данных"**

     Вы можете использовать этот параметр, чтобы скрыть или отобразить раздел **Операции** → **Шифрование и защита данных** в интерфейсе. Kaspersky Security Center Cloud Console сохраняет значение этого параметра только для вашей учетной записи; при этом другой пользователь может установить другое значение.

   - **Показать функции MDR**

     Вы можете использовать этот параметр, чтобы скрыть или отобразить раздел **Мониторинг** → **Инциденты** в интерфейсе. Kaspersky Security Center Cloud Console сохраняет значение этого параметра только для вашей учетной записи; при этом другой пользователь может установить другое значение.
3. Укажите количество устройств, которое Kaspersky Security Center Cloud Console будет отображать в результатах распространения политики.
4. Нажмите на кнопку **Сохранить**.

Параметры интерфейса настроены в соответствии с вашими требованиями.

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.

Чтобы создать и добавить виртуальный Сервер администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.
2. На открывшейся странице выберите вкладку **Серверы администрирования**.
3. Выберите группу администрирования, в которую вы хотите добавить виртуальный Сервер администрирования.
4. В меню выберите пункт **Новый виртуальный Сервер администрирования**.
5. На открывшейся странице укажите **Имя виртуального Сервера администрирования**.
6. Нажмите на кнопку **Сохранить**.

Новый виртуальный Сервер администрирования создан, добавлен в группу администрирования и отображается на вкладке **Серверы администрирования**.

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 администратор не включен в список **Права доступа** в свойствах главного Сервера 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.

При назначении администратора убедитесь, что вы предоставляете доступ к одному виртуальному Серверу администрирования. Администратор, имеющий доступ к нескольким виртуальным Серверам администрирования, не может войти в Kaspersky Security Center Cloud Console.

Администратор виртуального Сервера администрирования входит в Kaspersky Security Center Cloud Console так же, как и на главный Сервер администрирования. Kaspersky Security Center Cloud 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.
- Созданная учетная запись администратора виртуального Сервера не включается в список **Права доступа** в свойствах любых Серверов, главных и подчиненных.
- 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 **ОК**.

   Приложение добавляет выбранного пользователя в список пользователей на вкладку **Права доступа**.

5. Установите флажок рядом с добавленной учетной записью и нажмите на кнопку **Права доступа**.

6. Настройте права администратора на виртуальном Сервере администрирования.

   Для успешной аутентификации администратор должен иметь следующие права:

   - 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 нескольких виртуальных Серверов администрирования:

1. В главном окне приложения нажмите на имя основного Сервера администрирования.

2. На открывшейся странице перейдите на вкладку **Права доступа** и нажмите на кнопку **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**.

   При выборе двух и более виртуальных серверов доступ к их основному Серверу администрирования будет предоставлен автоматически. В этом случае выбор невозможно будет отменить, не отменяя выбор соответствующих виртуальных серверов.

6. Выберите роли администратора, которые вы хотите назначить пользователю, если это необходимо.

   Если вы хотите назначить пользовательские роли для текущего Сервера администрирования, перейдите в свойства этого Сервера администрирования, нажмите **Назначить роли** и выберите пользовательские роли.

7. Нажмите на кнопку **Готово**, чтобы применить 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 выберите 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.

   > При назначении ролей пользователю, в главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**. Если вы выберете вкладку **Группы** и назначите роли группе, членом которой является пользователь, пользователь не сможет войти в Kaspersky Security Center Cloud Console.

Приложение назначает новую 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.

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 Cloud Console, выполните опрос сети, а затем переместите найденные устройства из группы Нераспределенные устройства в группы администрирования.

Чтобы удалить виртуальный Сервер администрирования:

1. В главном окне приложения нажмите на Сервер администрирования.
2. На открывшейся странице перейдите на вкладку **Серверы администрирования**.
3. Выберите виртуальный Сервер администрирования, который вы хотите удалить.
4. В строке меню нажмите на кнопку **Удалить**.

Виртуальный Сервер администрирования удален.

Мониторинг и отчеты

В этом разделе описаны функции мониторинга и работа с отчетами в Kaspersky Security Center Cloud Console. Эти функции позволяют получать сведения об инфраструктуре вашей сети, статусе защиты, а также статистику.

В процессе развертывания или во время работы Kaspersky Security Center Cloud Console можно настраивать функции мониторинга и параметры отчетов.

Сценарий: мониторинг и отчеты

В этом разделе представлен сценарий настройки мониторинга и отчетов в Kaspersky Security Center Cloud Console.

Предварительные требования

После развертывания Kaspersky Security Center Cloud Console в сети организации вы можете приступить к мониторингу состояния безопасности сети с помощью Kaspersky Security Center и к формированию отчетов.

Этапы

Настройка мониторинга и работы с отчетами в сети организации состоит 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 параметров уведомлений (по электронной почте) о событиях на клиентских устройствах.

   > Рекомендуется настроить автоматическую пересылку событий в SIEM-систему для долговременного хранения событий приложений "Лаборатории Касперского". Это также позволяет оперативно получать уведомления по электронной почте о событиях информационной безопасности и быстрее реагировать на них.

3. **Изменение ответа вашей сети безопасности на событие Вирусная атака**

Вы можете изменить пороговые значения в свойствах Сервера администрирования. Вы также можете создать более строгую политику, которая будет активирована, или создать задачу, которая будет запускаться при возникновении этого события.

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. **Просмотр информации о лицензии**

   Инструкции:

   - Добавление виджета **Используемые лицензионные ключи** на панель мониторинга и его просмотр.
   - Генерация и просмотр отчета **Отчет об использовании лицензионных ключей**.

Результаты

После завершения сценария вы будете проинформированы о защите сети вашей организации и, таким образом, сможете планировать действия для дальнейшей защиты.

О типах мониторинга и отчетах

Информация о событиях безопасности в сети организации хранится в базе данных Сервера администрирования. Kaspersky Security Center Cloud Console предоставляет следующие виды мониторинга и отчетов, основанные на событиях в сети вашей организации:

- Панель мониторинга
- Отчеты
- Выборки событий

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 Cloud Console.

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 Cloud 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 Cloud 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**.
2. Нажмите на кнопку **Добавить или восстановить виджет**.

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.

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.
3. Выберите **Скрыть виджет**.
4. В открывшемся окне **Предупреждение** нажмите на кнопку **ОК**.

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 Cloud Console (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 **Modify object ACLs** 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 на 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 Cloud Console, 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 Cloud Console 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 Cloud Console в разделе **Мониторинг → Отчеты**.

По умолчанию отчеты включают информацию за последние 30 дней.

Kaspersky Security Center Cloud Console 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.
4. На шаге мастера **Область действия** выберите набор клиентских устройств (групп администрирования, выборок устройств или всех сетевых устройств), данные о которых будут отображаться в отчетах, сформированных на основе этого шаблона.
5. На шаге мастера **Период отчета** укажите период, за который будет формироваться отчет. Доступные значения:

   - между двумя указанными датами;
   - от указанной даты до даты создания отчета;
   - от даты создания отчета минус указанное количество дней до даты создания отчета.

   В некоторых отчетах эта страница может не отображаться.
6. Нажмите на кнопку **ОК**, чтобы завершить работу мастера.
7. Выполните одно из следующих действий:

   - Нажмите на кнопку **Сохранить и запустить**, чтобы сохранить новый шаблон отчета и запустить формирование отчета на его основе.

     Шаблон отчета будет сохранен. Отчет будет сформирован.
   - Нажмите на кнопку **Сохранить**, чтобы сохранить новый шаблон отчета.

     Шаблон отчета будет сохранен.

Созданный шаблон можно использовать для формирования и просмотра отчетов.

Просмотр и изменение свойств шаблона отчета

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**.
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.

       Интерфейс Kaspersky Security Center Cloud Console может отображать не более 2500 записей. Если вам нужно просмотреть большее количество событий, воспользуйтесь функцией экспорта отчета.

     - **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 Cloud Console 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.

3. Нажмите на кнопку **Экспортировать отчет**.

4. В открывшемся окне укажите 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.

- **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.

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 только на английском языке, другие локализации недоступны.

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>).

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**.

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 каждый понедельник 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**.

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 выключен.

  - **Использовать автоматическое определение случайного интервала между запусками задачи**

    Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

    Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

    Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  - **Использовать 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.

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.

    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 **ОК**, чтобы подтвердить свой выбор.

Выбранные шаблоны отчетов будут удалены. Если эти шаблоны отчетов были включены в задачи рассылки отчетов, они также будут удалены из этих задач.

События и выборки событий

В этом разделе содержится информация о событиях и выборках событий, о типах событий, возникших в компонентах Kaspersky Security Center Cloud Console, и об управлении блокировкой частых событий.

О событиях в Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console 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 экспортировать эту информацию во внешние SIEM-системы. Экспорт информации о событиях во внешние SIEM-системы позволяет администраторам SIEM-систем оперативно реагировать на события системы безопасности, произошедшие на управляемых устройствах или группах устройств.

События по типу

В Kaspersky Security Center Cloud Console 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 Cloud Console:
  - 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 Cloud Console. 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 Cloud Console

Каждый компонент Kaspersky Security Center Cloud Console имеет собственный набор типов событий. В этом разделе перечислены типы событий, которые происходят на Сервере администрирования Kaspersky Security Center Cloud Console 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 Cloud Console, 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 Cloud Console.
- **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.

События Сервера администрирования

В этом разделе содержится информация о событиях Сервера администрирования.

Критические события Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center Cloud Console 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.

Критические события Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Лицензионное ограничение превышено	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Один раз в день Kaspersky Security Center Cloud Console проверяет, не превышено ли лицензионное ограничение. 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 Cloud Console определяет правила генерации событий при превышении лицензионного ограничения.	180 дней
Вирусная атака	26 (для компонента Защита от файловых угроз)	GNRL_EV_VIRUS_OUTBREAK	События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения. 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.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Вирусная атака	27 (для компонента Защита от почтовых угроз)	GNRL_EV_VIRUS_OUTBREAK	События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения. 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.	180 дней
Вирусная атака	28 (для сетевого экрана)	GNRL_EV_VIRUS_OUTBREAK	События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения. 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.	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
Режим ограниченной функциональности	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	События этого типа возникают, если Kaspersky Security Center Cloud Console 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 Cloud Console (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 лицензии скоро истекает	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	События этого типа возникают, если приближается дата окончания срока действия коммерческой лицензии. Один раз в день Kaspersky Security Center проверяет, не истек ли срок действия лицензии. События этого типа публикуются за 30 дней, 15 дней, 5 дней и 1 день, до истечения срока действия лицензии. Это количество дней 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 Cloud Console работает в режиме Базовой функциональности. Вы можете ответить на событие следующими способами: • Убедитесь, что резервный лицензионный ключ добавлен на Сервер администрирования. • Если вы используете подписку, продлите ее. Неограниченная подписка продлевается автоматически, если предоплата поставщику услуг была своевременно внесена.	180 дней
Срок действия MDM-сертификата истек	4132	KLSRV_CERTIFICATE_EXPIRED	События этого типа возникают, если истек срок действия клиентского сертификата на мобильных устройствах.	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 экспертами "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 Cloud Console и не относится к модулям управляемых приложений "Лаборатории Касперского". Событие содержит причину, из-за которой обновления не установлены.	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

События отказа функционирования Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center Cloud Console 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
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 Cloud Console вы управляете лицензионными ключами приложений сторонних производителей и если количество установок превысило заданное в лицензионном ключе приложения стороннего производителя ограничение. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите приложение стороннего производителя с устройств, на которых оно не используется. • Используйте лицензию стороннего производителя на большее количество устройств. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений. В группу лицензионных приложений входят приложения сторонних производителей, отвечающие заданным вами критериям.	180 дней
Не удалось выполнить 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

События предупреждения Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center Cloud Console 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.

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Лицензионное ограничение превышено	4098	KLSRV_EV_LICENSE_CHECK_100_110	Один раз в день Kaspersky Security Center Cloud Console проверяет, не превышено ли лицензионное ограничение. 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 Cloud Console определяет правила генерации событий при превышении лицензионного ограничения.	90 дней
Устройство долго не проявляет активности в сети	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	События этого типа возникают, если управляемое устройство неактивно в течение некоторого времени. Чаще всего это происходит, когда управляемое устройство выводится из эксплуатации. Вы можете ответить на событие следующими способами: • Удалите устройство из списка управляемых устройств вручную. Укажите интервал, по истечении которого создается событие **Устройство долго не проявляет активности в сети** с помощью Kaspersky Security Center Cloud Console. • Укажите интервал, по истечении которого устройство автоматически удаляется из группы с помощью Kaspersky Security Center Cloud Console.	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. Хотя клонирование не поддерживается в Kaspersky Security Center Cloud Console, это событие может произойти, если вы выполняете клонирование с использованием стороннего инструмента. Чтобы избежать этого события, при копировании образа устройства с установленным Агентом администрирования необходимо соблюдать следующие рекомендации: • На эталонном устройстве остановить службу Агента администрирования и запустить утилиту klmover с ключом -dupfix. В дальнейшем не допускать запуск службы Агента администрирования вплоть до выполнения операции захвата образа. • Обеспечен запуск утилиты klmover с ключом -dupfix до (это важно) первого запуска службы Агента администрирования на устройствах при первом старте операционной системы после развертывания образа. Утилита klmover входит в состав инсталляционного пакета Агента администрирования. Если вы захватываете образ устройства без установленного Агента администрирования, нужно развернуть образ на целевых устройствах, а затем установить Агент администрирования. Также требуется предоставить доступ к сетевой папке с автономными инсталляционными пакетами с устройства.	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

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	4127	KLSRV_INVLICPROD_FILLED	События этого типа возникают, если количество установок приложений сторонних производителей, включенных в группу лицензионных приложений, достигает 90% от максимально допустимого значения, указанного в свойствах лицензионного ключа. Вы можете ответить на событие следующими способами: • Если приложение стороннего производителя не используется на каких-то управляемых устройствах, удалите приложение с этих устройств. • Если вы ожидаете, что количество установок для приложения стороннего производителя превысит разрешенное ограничение в ближайшем будущем, рассмотрите возможность получения лицензии приложения стороннего производителя на большее количество устройств заранее. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений.	90 дней
Сертификат запрошен	4133	KLSRV_CERTIFICATE_REQUESTED	События этого типа возникают, если не удается автоматически перевыпустить сертификат для Управления мобильными устройствами. Ниже приведены возможные причины событий и соответствующие действия по реагированию на событие: • Автоматический перевыпуск был инициирован для сертификата, для которого параметр **Сертификат запрошен**. Это могло произойти из-за ошибки, которая возникла при создании сертификата. Может потребоваться перевыпуск сертификата вручную. • Если вы используете интеграцию с инфраструктурой открытых ключей, причиной может быть отсутствие атрибута SAM-Account-Name учетной записи, которая используется для интеграции с PKI и для выпуска сертификата. Просмотрите свойства учетной записи.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Сертификат удален	4134	KLSRV_CERTIFICATE_REMOVED	События этого типа возникают, если администратор удаляет сертификат любого типа (общий, почтовый, VPN) для Управления мобильными устройствами. После удаления сертификата мобильные устройства, подключенные по этому сертификату, не смогут подключиться к Серверу администрирования. Это событие может быть полезно при исследовании неисправностей, связанных с Управлением мобильными устройствами.	90 дней
Срок действия APNs-сертификата истек	4135	KLSRV_APN_CERTIFICATE_EXPIRED	События этого типа происходят, если истекает срок действия APNs-сертификата. Вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM.	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.	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

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
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
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
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
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
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
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
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 Kaspersky Security Center Cloud Console 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.

Информационные события Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
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 Cloud Console определяет правила генерации событий при превышении лицензионного ограничения.	30 дней
Обнаружено новое устройство	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	События этого типа возникают при обнаружении новых сетевых устройств.	30 дней
Устройство было автоматически перемещено с помощью правила	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	События этого типа возникают, если устройства были отнесены к группе в соответствии с правилами перемещения устройств.	30 дней
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.	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Для одной из групп лицензионных приложений число разрешенных установок исчерпано более чем на 90%	4128	KLSRV_INVLICPROD_EXPIRED_SOON	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.	30 дней
Появились файлы для отправки на анализ в "Лабораторию Касперского"	4131	KLSRV_APS_FILE_APPEARED		30 дней
Идентификатор экземпляра FCM мобильного устройства изменен	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	События этого типа возникают при изменении токена Firebase Cloud Messaging на устройстве. Информацию о ротации токенов FCM см. в документации сервиса Firebase.	30 дней
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.	30 дней
Установлено соединение с подчиненным Сервером администрирования	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	Подробнее см. в статье Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования.	30 дней
Установлено соединение с главным Сервером администрирования	4117	KLSRV_EV_MASTER_SRV_CONNECTED		30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Базы обновлены (В Kaspersky Security Center Cloud Console этот тип событий доступен только для подчиненного Сервера администрирования.)	4144	KLSRV_UPD_BASES_UPDATED	События этого типа возникают, когда задача **Загрузка обновлений в хранилище Сервера администрирования** завершает обновление базы данных.	30 дней
Устройство автоматически добавлено в группу	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	События этого типа возникают, если устройства были отнесены к группе в соответствии с правилами перемещения устройств.	30 дней
Прокси-сервер KSN был запущен; проверка доступности KSN прошла успешно	7718	KSNPROXY_STARTED_CON_CHK_OK		30 дней
Прокси-сервер KSN остановлен	7720	KSNPROXY_STOPPED		30 дней
Аудит: Подключение к Серверу администрирования	4147	KLAUD_EV_SERVERCONNECT		30 дней
Аудит: Подключение к Серверу администрирования было прервано	4151	KLAUD_EV_SERVERDISCONNECT		30 дней
Аудит: Изменение объекта	4148	KLAUD_EV_OBJECTMODIFY	Это событие отслеживает изменения в следующих объектах: • группах администрирования; • группах безопасности; • пользователях; • инсталляционных пакетах; • задачах; • политиках; • Серверах; • виртуальных Серверах.	30 дней
Аудит: Свойства объекта были изменены	4152	KLAUD_EV_OBJECTPROPMODIFIED	Это событие отслеживает изменения в следующих параметрах: • пользователь; • лицензия; • Сервер; • виртуальный Сервер.	30 дней
Аудит: Изменение статуса объекта	4150	KLAUD_EV_TASK_STATE_CHANGED	Например, это событие возникает, если задача завершилась ошибкой.	30 дней
Аудит: Изменение параметров группы	4149	KLAUD_EV_ADMGROUP_CHANGED	События этого типа возникают при изменении группы безопасности.	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Аудит: Импорт или экспорт ключей шифрования с Сервера администрирования	5100	KLAUD_EV_DPEKEYSEXPORT		30 дней
Аудит: Тестовое подключение к SIEM-серверу выполнено успешно	5110	KLAUD_EV_SIEM_TEST_SUCCESS		30 дней
Аудит: Права пользователя были изменены	4153	KLAUD_EV_OBJECTACLMODIFIED	События этого типа возникают, если права пользователя были изменены.	30 дней

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 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.

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 Cloud Console 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
Не удалось установить обновление стороннего производителя	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	События этого типа возникают, если используются возможности Системного администрирования и Управления мобильными устройствами, 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 Центра обновления Windows	7717	KLNAG_EV_WUA_INSTALL_ERROR	События этого типа возникают, если обновления Центра обновления Windows были неуспешными. Настройте обновления Microsoft Windows в политике Агента администрирования. 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 установить корневые сертификаты	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	Событие содержит описание ошибки установки сертификатов.	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
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 Kaspersky Security Center с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. 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	Срок хранения по умолчанию
Возвращено предупреждение во время установки обновления модулей приложений	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 дней
Установка обновления стороннего ПО завершена с предупреждением	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 дней
Установка обновления стороннего программного обеспечения отложена	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 дней
Произошла проблема безопасности	549	GNRL_EV_APP_INCIDENT_OCCURED	30 дней
Обнаружен файл sudoers, который не соответствует референсному значению	7724	KLNAG_EV_SUDOER_DIFFERENT	30 дней
Прокси-сервер KSN был запущен. Не удалось проверить доступность KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 дней
Управление учетными записями: предупреждения	7722	KLNAG_EV_USR_MNG_WRN	30 дней

Информационные события Агента администрирования

В таблице ниже приведены события Агента администрирования Kaspersky Security Center с уровнем важности **Информационное сообщение**.

Для каждого события, которое может генерировать 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
Обновление модулей приложений успешно установлено	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 дней
Запущена установка обновления модулей приложений для программного обеспечения	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 дней
Установлено приложение	7703	KLNAG_EV_INV_APP_INSTALLED	30 дней
Приложение удалено	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 дней
Установлено наблюдаемое приложение	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 дней
Удалено наблюдаемое приложение	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 дней
Установлено стороннее приложение	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	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
Новое устройство добавлено	7708	KLNAG_EV_DEVICE_ARRIVAL	30 дней
Устройство удалено	7709	KLNAG_EV_DEVICE_REMOVE	30 дней
Обнаружено устройство	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Устройство авторизовано	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	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
Получен сертификат для HTTPS-порта Веб-сервера	—	WEB_SERVER_CERTIFICATE_RENEWED	30 дней
Совместный доступ к рабочему столу Windows: файл был прочитан	7712	KLUSRLOG_EV_FILE_READ	30 дней
Совместный доступ к рабочему столу Windows: файл был изменен	7713	KLUSRLOG_EV_FILE_MODIFIED	30 дней
Совместный доступ к рабочему столу Windows: приложение было запущено	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	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
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
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

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 Cloud Console.

Выборки событий доступны в Kaspersky Security Center Cloud Console в разделе **Мониторинг → Выборки событий**.

По умолчанию выборки событий включают информацию за последние семь дней.

Kaspersky Security Center Cloud Console имеет набор выборок (предопределенных) по умолчанию:

- События с разным уровнем важности:
  - **Критические события.**
  - **Отказ функционирования.**
  - **Предупреждения.**
  - **Информационные сообщения.**
- **Запросы пользователей** (события управляемых приложений).
- **Последние события** (за последнюю неделю).
- **События аудита.**

  В Kaspersky Security Center Cloud Console события аудита, связанные со служебными операциями, отображаются в вашей рабочей области. Эти события обусловлены действиями специалистов "Лаборатории Касперского". Такие события, например, включают: изменение портов Сервера администрирования; резервное копирование данных Сервера администрирования; создание, изменение и удаление учетных записей пользователей.

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 Cloud Console 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**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Новая выборка событий** укажите параметры новой выборки событий. Параметры можно указать в нескольких разделах этого окна.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

   Откроется окно подтверждения.
5. Чтобы просмотреть результат выборки событий, установите флажок **Перейти к 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.
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 редактировать все свойства.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененная выборка событий отображается в списке.

Просмотр списка выборки событий

Просмотр выборки событий:

1. В главном окне приложения перейдите в раздел **Мониторинг → Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется запустить.
3. Выполните одно из следующих действий:
   - Чтобы настроить сортировку для результатов выборки событий:
     a. Нажмите на кнопку **Изменить сортировку и запустить**.
     b. В отобразившемся окне **Изменить сортировку для выборки событий** укажите параметры сортировки.
     c. Нажмите на имя выборки.
   - В противном случае, если вы хотите просмотреть список событий так, как они хранятся на Сервере администрирования, нажмите на название выборки.

Отобразится результат выборки событий.

Экспорт выборки событий

Kaspersky Security Center Cloud Console 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 Cloud Console (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 Cloud Console 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**.
3. В открывшемся окне можно выполнить следующие действия:
   - Просмотреть информацию выбранного события.
   - Перейти к следующему или к предыдущему событию в списке – результате выборки событий.
   - Перейти к устройству, на котором возникло событие.
   - Перейти к группе администрирования, содержащей устройство, на котором возникло событие.
   - Для события, связанного с задачей, перейдите в свойства задачи.

Экспорт событий в файл

Kaspersky Security Center Cloud Console позволяет сохранять события из выборки событий в файл TXT.

Чтобы экспортировать события в файл:

1. Запустите выборку событий.
2. Установите флажок рядом с требуемым событием.

   Вы также можете выбрать несколько событий или всю выборку событий.
3. Нажмите на кнопку **Экспортировать в файл**.

Выбранные события будут экспортированы в файл формата TXT.

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.

Хранение информации о событиях для задач и политик

В этом разделе приведены рекомендации, как минимизировать количество событий для задач и политик, хранящихся в базе данных Kaspersky Security Center Cloud Console. Если превышено ограничение хранилища, новые события перезаписывают старые. В результате критические события могут исчезнуть. Так же могут возникнуть события предупреждения Сервера администрирования, которые называются **Превышено ограничение числа событий, удалены события из базы данных**. В этих случаях рекомендуется следовать инструкциям в этом разделе.

В результате повысится скорость выполнения сценариев, связанных с анализом событий. Также эти рекомендации помогут снизить риск того, что критические события будут перезаписаны большим количеством событий.

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 часто (например, более одного раза в неделю), 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 Kaspersky Security Center Cloud Console сохраняет с каждого устройства, на котором выполнена задача, в базу данных только информацию о запуске задачи, о ее ходе и о ее выполнении (успешном, с предупреждением либо с ошибкой).

- **Сохранять только результат выполнения задачи**. В этом случае Kaspersky Security Center Cloud Console сохраняет с каждого устройства, на котором выполнена задача, в базу данных только информацию 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 этом случае рекомендуется выбрать в свойствах политики только наиболее важные события и включить их сохранение. Сохранение всех других событий рекомендуется отключить.

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.

Изменить параметры хранения событий целесообразно, если события об изменении промежуточных статусов групповых задач и события о применении политик занимают большую долю всех событий в базе данных Kaspersky Security Center Cloud Console.

Удаление событий

Чтобы удалить события из выборки событий:

1. Запустите выборку событий.

2. Выберите следующие 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**.

Чтобы удалить события из списка событий устройства:

1. Откройте список устройств.
   - Для управляемых устройств: **Управление активами** → **Активы (Устройства)**.
   - Нераспределенные устройства: **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.
2. В списке устройств нажмите на ссылку с названием нужного устройства и перейдите на вкладку **События**.
3. Выберите следующие 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 **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.

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 Windows, 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 меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Заблокированные частые события**.

3. В разделе **Заблокированные частые события**:

   - 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 **Заблокировано**.

  b. Нажмите на кнопку **Сохранить**.

Сервер администрирования принимает разблокированные частые события и не принимает заблокированные частые события.

Отмена блокировки частых событий

Вы можете отменить блокировку частых событий и начать получение событий до тех пор, пока Сервер администрирования снова не заблокирует эти частые события.

Чтобы отменить блокировку частых событий:

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

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Заблокированные частые события**.

3. В разделе **Заблокированные частые события** 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.

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.
- Уведомления по электронной почте.

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** или **Информационное сообщение**.

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 Cloud Console 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.

Kaspersky Security Center Cloud Console позволяет вам контролировать сеть вашей организации, отправляя уведомления о событиях, которые вы считаете важными. Для любого события вы можете настроить уведомление электронной почте.

Получив уведомление по электронной почте, вы можете принять решение о своем ответе на событие. Этот ответ должен быть наиболее подходящим для сети вашей организации.

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 Cloud Console 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 Cloud Console и устанавливают разные языки интерфейса, Kaspersky Security Center Cloud Console 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 Cloud Console.

  Для предоставления информации, которая соответствует вашей конфигурации защиты сети, Kaspersky Security Center Cloud Console 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 Cloud Console.

- 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 Cloud Console 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

Объявления включают два типа информации:

- Объявления, связанные с безопасностью.
- Рекламные объявления.

Вы можете выключить объявления каждого типа отдельно.

> Вы не можете отключить объявления, связанные с безопасностью, в пробном режиме Kaspersky Security Center Cloud Console.

Выключение объявлений, связанных с безопасностью

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 безопасности Выключены**.
4. Нажмите на кнопку **Сохранить**.

   Объявления, связанные с безопасностью, выключены.

Выключение маркетинговых объявлений

Рекламные объявления по умолчанию выключены. Вы получаете рекламные сообщения только в том случае, если вы включили Kaspersky Security Network (KSN). Вы можете выключить этот тип объявлений, отключив KSN.

Чтобы отключить объявления:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры KSN**.

3. Переведите переключатель в положение **Использовать Kaspersky Security Network Выключено**.

4. Нажмите на кнопку **Сохранить**.

   Объявления выключены.

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. 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 **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**.

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 **ОК**.

При выполнении заданных условий управляемому устройству присваивается статус *Предупреждение*.

Настройка параметров доставки уведомлений

Вы можете настроить уведомления по электронной почте о событиях, возникающих в Kaspersky Security Center Cloud Console.

Чтобы настроить параметры доставки уведомлений о событиях, возникших в Kaspersky Security Center Cloud Console:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Перейдите в раздел **Уведомление** и в правой панели задайте параметры уведомлений по электронной почте:

   Получатели (адреса электронной почты)

   Адреса электронной почты, на которые приложение Kaspersky Security Center Cloud Console будет отправлять уведомления. В этом поле можно указать несколько адресов через точку с запятой.

   Вы можете указать не более 24 адресов электронной почты.

3. Нажав на кнопку **Отправить тестовое сообщение** можно проверить правильно ли настроены сообщения: приложение отправляет тестовые сообщения на указанные адреса электронной почты.

4. Нажмите на кнопку **OK**, чтобы закрыть окно свойств Сервера администрирования.

Сохраненные параметры доставки уведомлений применяются ко всем событиям, которые возникают в Kaspersky Security Center Cloud Console.

Можно изменить значения параметров доставки уведомлений для определенных событий в разделе **Настройка событий** в параметрах Сервера администрирования, параметрах политики или параметрах приложения.

Получение предупреждения об истечении срока лицензии

Чтобы добавить лицензионный ключ для Kaspersky Endpoint Security для бизнеса Стандартный на Сервер администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Лицензионные ключи**.

3. Нажмите на кнопку **Выбрать**.

4. В открывшемся окне выберите ваш файл ключа и нажмите на кнопку **OK**.

   Если лицензионный ключ не отображается, вы можете нажать на кнопку **Добавить лицензионный ключ**, и использовать свой код активации.

Файл ключа будет добавлен в хранилище Сервера администрирования. В этом случае Сервер администрирования генерирует критическое событие *Срок действия лицензии скоро истекает* за один день до истечения срока действия лицензии, а критическое событие *Режим ограниченной функциональности* после истечения срока действия лицензии. Вы можете настроить параметры доставки уведомлений.

Если вы добавляете лицензионный ключ для Kaspersky Endpoint Security для бизнеса Стандартный в хранилище Сервера администрирования, то этот лицензионный ключ считается использованным на одном устройстве.

Cloud Discovery

Kaspersky Security Center Cloud Console 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 Cloud Console по лицензии Kaspersky Next EDR Optimum или Kaspersky Security для бизнеса Профессиональный.

Возможность блокировки доступна только при использовании Kaspersky Endpoint Security 11.2 для Windows и более поздних версий. 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 Kaspersky, предоставляющую 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 Cloud Console получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных политиками безопасности или профилями политик, в которых она включена.

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 Cloud Console.
2. В главном окне приложения перейдите в раздел **Мониторинг → Панель мониторинга**.
3. В виджете **Cloud Discovery** нажмите на кнопку **Включить**.
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 Cloud Console.
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 веб-виджета.

Выбранный виджет будет добавлен в конец панели мониторинга.

Просмотр информации об использовании облачных сервисов

Вы можете просмотреть виджет **Cloud Discovery**, на котором отображается информация о попытках получить доступ к облачным службам. Виджет также показывает уровень риска каждого облачного сервиса. Kaspersky Security Center Cloud Console получает информацию об использовании облачных сервисов со всех управляемых устройств, защищенных только теми профилями безопасности, в которых эта функция включена.

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 Cloud Console.
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 Cloud Console по лицензии Kaspersky Next EDR Optimum или Kaspersky Security для бизнеса Профессиональный.

Возможность блокировки доступна только при использовании Kaspersky Endpoint Security 11.2 для Windows и более поздних версий. 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, уровень риска можно учесть 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 веб-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.

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 **Операции** → **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 Cloud Console 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 Cloud Console 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 **Операции** → **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 **Операции** → **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**.

Использование Kaspersky Security Center Cloud Console 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 Cloud Console, 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 Cloud Console 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.

После активации Сервера администрирования по лицензии Kaspersky Security для бизнеса Профессиональный и распространении лицензионного ключа на управляемые приложения, вы можете выполнять 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.

Также вы можете использовать функциональность Kaspersky Security для бизнеса Профессиональный в пробном режиме. Для этого в пробном режиме вам нужно создать пробную рабочую область, а затем распространить пробный лицензионный ключ на ваши управляемые приложения. Функциональность Kaspersky Security для бизнеса Профессиональный будет доступна в течение срока действия пробной рабочей области.

Интеграции для реагирования на алерты

Вы можете настроить интеграции со следующими решениями для реагирования на угрозы:

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

Чтобы настроить интеграции, требуется выполнение следующих условий:

- При использовании функциональности Kaspersky Security для бизнеса Профессиональный в коммерческом режиме, вам нужно:
  - Иметь коммерческую рабочую область и права **Чтение** и **Запись** для функциональной области **Общие функции: Интеграция приложения**.
  - Активировать Сервер администрирования по лицензии Kaspersky Security для бизнеса Профессиональный.
  - Распространить лицензионный ключ Kaspersky Security для бизнеса Профессиональный на управляемые приложения для выполнения действий по реагированию.

  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 лицензионного ключа на подчиненные и виртуальные Серверы администрирования не поддерживается.

- При использовании функциональности Kaspersky Security для бизнеса Профессиональный в пробном режиме, вам нужно создать пробную рабочую область, а затем распространить пробный лицензионный ключ на ваши управляемые приложения. Функциональность Kaspersky Security для бизнеса Профессиональный будет доступна в течение срока действия пробной рабочей области.

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.

Интеграция с Active Directory для реагирования на алерты, ADFS-интеграция и параметры проверки контроллера домена Active Directory (адрес и учетные данные пользователя контроллера домена), который вы указываете при настройке опроса контроллера домена, это разные параметры. 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. Выберите раздел **Точки распространения**, нажмите на название нужной точки распространения.

3. В открывшемся окне свойств выберите раздел **Шлюз соединения** и включите параметр **Шлюз соединения**.

4. Выберите раздел **Active Directory**.

5. 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.

6. Создайте соединение к контроллеру домена Active Directory, нажав на кнопку **Добавить соединение**.

7. В открывшемся окне настройте следующие параметры для соединения:

   - **Адрес контроллера домена**

     Имя компьютера, например: `server.example.com`.

     Вы можете указать несколько IP-адресов. Все контроллеры домена, IP-адреса которых вы указываете, должны принадлежать одному домену.

   - **Доменное имя Active Directory.**

     Полное доменное имя DNS, например: `example.com`.

     Также вы можете указать SAM-имя или NetBIOS-имя, например: `example`.

     Используйте строчные буквы. Если вы создаете несколько соединений для Сервера администрирования или точки распространения, укажите разные имена для каждого соединения.

     > Не рекомендуется использовать адрес конкретного контроллера домена и короткое имя домена (SAM или NetBIOS).
     > 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.

8. Если вы хотите проверить статус соединения, нажмите на кнопку **Проверить соединение**.

   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. 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.

9. Нажмите на кнопку **Создать**.

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 Cloud 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. В разделе **Интеграции** выберите **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.

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. 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

В коммерческом режиме, чтобы включить функционал агрегации алертов, необходимо активировать Сервер администрирования по лицензии Kaspersky Security для бизнеса Профессиональный, а затем распространить лицензионный ключ Kaspersky Security для бизнеса Профессиональный на управляемые приложения. 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.

В пробном режиме у вас должна быть пробная рабочая область и вам нужно распространить пробный лицензионный ключ на ваши управляемые приложения. Функция агрегирования алертов будет доступна в течение срока действия вашей пробной рабочей области.

Агрегация алертов в группы, которые могут относиться к одному инциденту, что упрощает процесс расследования. 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.

Удаленная диагностика клиентских устройств

Вы можете использовать удаленную диагностику для удаленного выполнения следующих операций на клиентских устройствах на базе Windows и на базе Linux:

- включения и выключения трассировки, изменения уровня трассировки и загрузки файла трассировки;
- загрузки системной информации и параметров приложения;
- загрузки журналов событий;
- создание файла дампа для приложения;
- запуска диагностики и загрузки результатов диагностики;
- запуск, остановка и перезапуск приложений.

Вы можете использовать журнал событий и диагностические отчеты, загруженные с клиентского устройства, для устранения неполадок самостоятельно. Также если вы обращаетесь в Службу технической поддержки "Лаборатории Касперского", эксперт 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** → **Активы (Устройства)**.
   - Если устройство принадлежит к группе нераспределенных устройств, в главном меню перейдите в раздел **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.
2. Нажмите на имя требуемого устройства.
3. В открывшемся окне свойств устройства выберите вкладку **Дополнительно**.
4. 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 дереве объектов устройства 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 эксперт 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 Kaspersky Security Agent регулируется параметрами Агента администрирования. Поэтому параметры **Включить трассировку** и **Изменить уровень трассировки** выключены для этого компонента на клиентских устройствах под управлением Linux.

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 эксперты 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 эксперта 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

Вы можете загрузить файлы трассировки с клиентского устройства. только если выполняется одно из следующих условий: параметр **Не разрывать соединение с Сервером администрирования** включен в параметрах устройства, используется push-сервер или используется шлюз соединения. Иначе загрузка невозможна.

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

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 трассировки устройства**, где отображается список файлов трассировки.

5. В списке файлов трассировки выберите файл, который вы хотите загрузить.

6. Выполните одно из следующих действий:

   - Загрузите выбранный файл, нажав на кнопку **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.

   Откроется окно **Журналы трассировки устройства**, где отображается список файлов трассировки.

4. В списке файлов трассировки выберите один или несколько файлов, которые вы хотите удалить.

5. Нажмите на кнопку **Удалить**.

Выбранные файлы трассировки удалены.

Загрузка параметров приложений

Вы можете загрузить параметры приложений с клиентского устройства только если выполняется одно из следующих условий: параметр **Не разрывать соединение с Сервером администрирования** включен в параметрах устройства, используется push-сервер или используется шлюз соединения. Иначе загрузка невозможна.

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

Чтобы загрузить с клиентского устройства параметры программ:

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

Вы можете загрузить системную информацию с клиентского устройства на свое устройство только если выполняется одно из следующих условий: параметр **Не разрывать соединение с Сервером администрирования** включен в параметрах устройства, используется push-сервер или используется шлюз соединения. Иначе загрузка невозможна.

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

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.

> 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

Вы можете загружать журналы событий с клиентского устройства на свое устройство только если выполняется одно из следующих условий: параметр **Не разрывать соединение с Сервером администрирования** включен в параметрах устройства, используется push-сервер или используется шлюз соединения. Иначе загрузка невозможна.

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

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.
     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 приложения и загрузка результатов

Чтобы запустить диагностику приложения 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 списке приложений выберите приложение, для которого вы хотите запустить удаленную диагностику.

   Откроется список параметров удаленной диагностики.
4. В разделе **Отчет диагностики** нажмите на кнопку **Выполнить диагностику**.

   Запускается процесс удаленной диагностики и генерируется отчет о диагностике. После завершения 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, который вы хотите запустить на клиентском устройстве. 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.

Создание файла дампа для приложения

Файл дампа приложения позволяет просматривать параметры приложения, работающего на клиентском устройстве, в определенный момент времени. Этот файл также содержит информацию о модулях, которые были загружены для приложения.

Создание файлов дампа доступно только для 32-разрядных процессов, работающих на клиентских устройствах под управлением Windows. Для клиентских устройств под управлением Linux и для 64-битных процессов эта функция не поддерживается.

Чтобы создать файл дампа для приложения:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Запуск удаленного приложения**.
3. В разделе **Формирование файла дампа процесса** укажите исполняемый файл приложения, для которого вы хотите создать файл дампа.
4. Нажмите на кнопку **Скачать**, чтобы сохранить файл дампа указанного приложения.

   Если указанное приложение не запущено на клиентском устройстве, отобразится сообщение об ошибке.

Запуск удаленной диагностики на клиентском устройстве с операционной системой Linux

Kaspersky Security Center Cloud Console позволяет загружать основную диагностическую информацию с клиентского устройства. Также 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 Cloud Console, вам нужно будет пройти все разделы интерфейса удаленной диагностики. Также 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 команду, чтобы распаковать архив collect.tar.gz:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Выполните 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.

Экспорт событий в SIEM-системы

В этом разделе описывается, как настроить экспорт событий в SIEM-системы.

Настройка экспорта событий в SIEM-системы

В этом разделе представлен сценарий настройки экспорта событий с Сервера администрирования во внешние SIEM-системы. Экспорт информации о событиях во внешние SIEM-системы позволяет администраторам SIEM-систем оперативно реагировать на события системы безопасности, произошедшие на управляемых устройствах или группах устройств.

Предварительные требования

Перед началом настройки экспорта событий в Kaspersky Security Center Cloud Console:

- Узнайте больше о методах экспорта событий.
- Убедитесь, что вам известны значения системных параметров.

Вы можете выполнять шаги этого сценария в любом порядке.

Этапы

Процесс экспорта событий в SIEM-систему состоит из следующих этапов:

- **Настройка SIEM-системы для получения событий из Kaspersky Security Center Cloud Console**

  Вам необходимо настроить получение событий из Kaspersky Security Center Cloud Console в SIEM-системе.

- **Выбор событий для экспорта**

  Вам нужно выбрать, какие события вы хотите экспортировать в SIEM-систему. Сначала отметьте общие события, которые происходят во всех управляемых приложениях "Лаборатории Касперского". Также можно отметить события для конкретных управляемых приложений "Лаборатории Касперского".

- **Настройка Kaspersky Security Center Cloud Console для экспорта событий в SIEM-систему**

  Вам необходимо настроить Kaspersky Security Center Cloud Console для начала экспорта событий в SIEM-систему.

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 Cloud Console необходимо указать некоторые параметры SIEM-системы. Рекомендуется уточнить эти параметры заранее, чтобы подготовиться к настройке Kaspersky Security Center Cloud Console.

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 Cloud Console и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky Security Center Cloud Console и настройках приемника в SIEM-системе.

- **Протокол**

  Протокол, используемый для передачи сообщений из Kaspersky Security Center Cloud Console в SIEM-систему. Это значение необходимо указать в настройках Kaspersky Security Center Cloud Console и настройках приемника в SIEM-системе.

Об экспорте событий

Kaspersky Security Center Cloud Console 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 Cloud Console во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center Cloud Console и получатель событий – SIEM-система. Для успешного экспорта событий необходимо выполнить настройки и в используемой SIEM-системе, и в Консоли администрирования Kaspersky Security Center Cloud Console. Последовательность настройки не имеет значения: Вы можете либо сначала настроить отправку событий в Kaspersky Security Center Cloud Console, а затем получение событий в SIEM-системе, либо наоборот.

Экспорт событий в формате Syslog

Вы можете отправлять события в формате syslog в любую SIEM-систему. Используя формат Syslog, вы можете передавать любые события, произошедшие на Сервере администрирования и в приложениях "Лаборатории Касперского", установленных на управляемых устройствах. При экспорте событий в формате Syslog можно выбирать, какие именно события будут переданы в SIEM-систему. Получение событий SIEM-системой

Получение событий SIEM-системой

SIEM-система должна принимать и корректно анализировать события, получаемые из Kaspersky Security Center Cloud Console. 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.

Настройка экспорта событий в SIEM-системе

В процедуре экспорта событий из Kaspersky Security Center Cloud Console во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center Cloud Console и получатель событий – SIEM-система. Экспорт событий необходимо настроить в используемой SIEM-системе и в Kaspersky Security Center Cloud Console.

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 Cloud Console. В общем случае в SIEM-системе необходимо указать следующие параметры:

- **Порт**

  Укажите номер порта для подключения к Kaspersky Security Center Cloud Console. Этот порт должен совпадать с портом, который вы указываете в Kaspersky Security Center Cloud Console при настройке экспорта событий в SIEM-систему.

- **Протокол передачи сообщений или тип исходных данных**

  Укажите формат Syslog.

В зависимости от используемой SIEM-системы может потребоваться указать дополнительные параметры приемника сообщений.

Анализатор сообщений

Экспортируемые события передаются в SIEM-систему в виде сообщений. Затем к этим сообщениям применяется анализатор, для того чтобы информация о событиях была должным образом передана в SIEM-систему. Анализатор сообщений встроен в SIEM-систему; он используется для разбиения сообщения на поля, такие как идентификатор сообщения, уровень важности, описание и прочие параметры. В результате SIEM-система имеет возможность выполнять обработку событий, полученных из Kaspersky Security Center Cloud Console, таким образом, чтобы они сохранялись в базе данных SIEM-системы.

Выбор событий для экспорта в SIEM-системы в формате syslog

После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться во внешнюю SIEM-систему.

Вы можете настроить экспорт событий в формате syslog во внешнюю систему на основе одного из следующих условий:

- Выбор общих событий. Если вы выберите экспортируемые события в политике, в свойствах события или в свойствах Сервера администрирования, то в SIEM-систему будут переданы выбранные события, которые произошли во всех 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.

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 → Активы (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. Выполните одно из следующих действий:

   - В главном окне приложения нажмите на имя Сервера администрирования.
   - В главном окне приложения перейдите в раздел **Управление активами** → **Политики**, а затем перейдите по ссылке политики.

2. В открывшемся окне выберите 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 Cloud Console во внешние системы.

В Kaspersky Security Center Cloud Console 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 Cloud Console таким образом, чтобы выполнялась отправка событий в SIEM-систему. Отправка событий из Kaspersky Security Center Cloud Console 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 Cloud Console для экспорта событий в SIEM-систему

Для экспорта событий в SIEM-систему необходимо настроить процесс экспорта в Kaspersky Security Center Cloud Console.

Чтобы настроить экспорт в SIEM-системы из Kaspersky Security Center Cloud Console:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Перейдите в раздел **SIEM** и нажмите ссылку **Параметры**.

3. На открывшейся правой панели **настройте параметры экспорта**.

   - В поле **Адрес сервера SIEM-системы** укажите IP-адрес сервера, на котором установлена используемая SIEM-система.

     Это значение необходимо уточнить в настройках SIEM-системы.

   - В поле **Порт SIEM-системы** укажите номер порта, по которому будет установлено соединение между Kaspersky Security Center Cloud Console и сервером SIEM-системы.

     Это значение необходимо указать в настройках Kaspersky Security Center Cloud Console и настройках приемника в SIEM-системе.

   - В списке **Протокол** значение выбрано по умолчанию. Вы можете использовать только TLS over TCP для передачи сообщений в SIEM-систему.

- В раскрывающемся списке **Аутентификация Сервера** выберите одно из следующих значений:

  - **Доверенные сертификаты**, а затем нажмите отобразившуюся кнопку **Выбрать файл центра сертификации** для загрузки доверенного сертификата.

    Вы можете получить полную цепочку сертификатов (включая корневой сертификат) от доверенного центра сертификации (CA) и загрузить его в Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console проверяет, подписана ли цепочка сертификатов SIEM-системы также доверенным центром сертификации или нет.

  - **Отпечатки SHA**, а затем в поле **Отпечатки** введите отпечаток SHA1 и нажмите на кнопку **Добавить**.

    Вы можете указать отпечатки SHA1 всей цепочки сертификатов SIEM-системы (включая корневой сертификат) в Kaspersky Security Center Cloud Console.

- Перейдите по ссылке **Добавить имя субъекта/альтернативное имя субъекта**.

  Эта ссылка отображается только в случае выбора пункта **Доверенные сертификаты** в раскрывающемся списке **Аутентификация Сервера**.

  Имя субъекта – это доменное имя, для которого получен сертификат. Kaspersky Security Center Cloud Console 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 **Имя субъекта/альтернативное имя субъекта**. Если какое-либо из указанных имен субъектов совпадает с именем субъекта сертификата SIEM-системы, Kaspersky Security Center Cloud Console проверяет сертификат сервера SIEM-системы.

- Перейдите по ссылке **Добавить проверку подлинности клиента**, а затем выберите в раскрывающемся списке **Если у вас нет сертификата, вы можете его сгенерировать** один из следующих вариантов:

  - **Сгенерировать ключ**, а затем нажмите на кнопку **Сгенерировать**, если требуется сгенерировать самоподписанный сертификат в Kaspersky Security Center Cloud Console. В результате Kaspersky Security Center Cloud Console сохраняет сгенерированный самоподписанный сертификат, и вы можете передать публичную часть сертификата или SHA1-отпечаток в SIEM-систему.

    С помощью этого параметра вы можете сгенерировать сертификат для аутентификации Kaspersky Security Center Cloud Console. Таким образом, вы будете использовать самоподписанный сертификат, выпущенный Kaspersky Security Center Cloud Console. В этом случае для аутентификации сервера SIEM-системы можно использовать как доверенный сертификат, так и отпечаток SHA.

  - **Вставить сертификат**, если вы хотите использовать сертификат, полученный из любого источника, например от любого аккредитованного центра сертификации.

    Затем укажите сертификат с соответствующим закрытым ключом, выполнив следующие действия:

    a. В раскрывающемся списке **Сертификация клиента** выберите тип сертификата:

    - **X.509-сертификат PEM**
    - **X.509-сертификат PKCS12**

    b. В поле **Файл с сертификатом** загрузите файл с сертификатом.

c. Если выбран вариант **X.509-сертификат PEM**, в отобразившемся разделе **Файл с ключом** загрузите файл с закрытым ключом.

Файл с сертификатом и файл с закрытым ключом не зависят друг от друга, и порядок загрузки этих файлов не важен.

d. Если закрытый ключ зашифрован, укажите пароль для расшифровки в поле **Проверка пароля или сертификата**. В противном случае это поле можно оставить пустым.

- В разделе **Формат данных** предварительно выбрано значение **Системный журнал**.

  Вы можете задать только ограничение длины сообщения, отправляемого в SIEM-систему, в поле **Максимальный размер сообщения в байтах**. В случае превышения этого предела сообщение будет обрезано.

4. 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 **OK**.

5. Переключите параметр в положение **Автоматически экспортировать события в базу SIEM-системы**.

6. Чтобы убедиться, что соединение с SIEM-системой настроено, нажмите на кнопку **Проверить подключение**.

   Отобразится статус подключения.

7. Нажмите на кнопку **Сохранить**.

Экспорт в SIEM-систему настроен. Если вы настроили получение событий в SIEM-системе, Сервер администрирования экспортирует выбранные события в SIEM-систему. Если вы установите дату начала экспорта, Сервер администрирования также экспортирует выбранные события, хранящиеся в базе данных Сервера администрирования, с указанной даты.

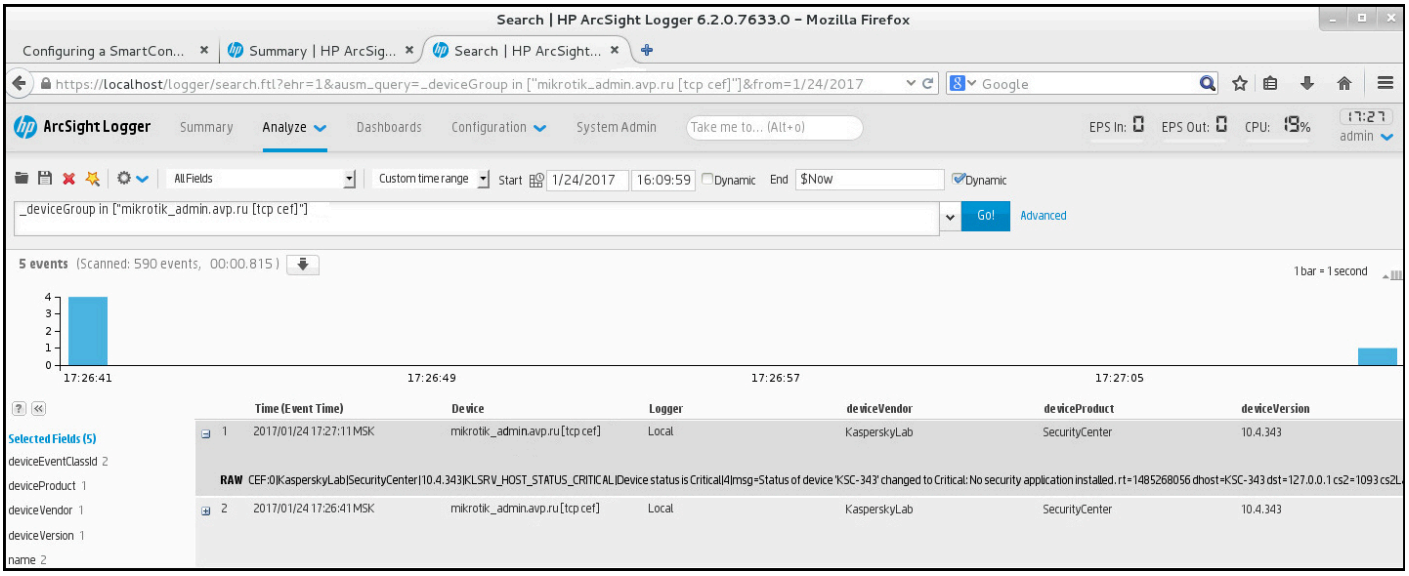
Просмотр результатов экспорта

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 Cloud Console 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 Cloud Console 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

Руководство по первоначальной настройке для поставщиков управляемых услуг (MSP)

Это краткое руководство предназначено для администраторов поставщиков услуг.

Kaspersky Security Center Cloud Console поддерживает мультитенантность. Руководство содержит советы и лучшие практики по управлению учетными записями ваших клиентов (тенантов) и установке приложений безопасности на их устройствах.

О Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console – это приложение, которое размещается и поддерживается "Лабораторией Касперского". Вам не нужно устанавливать Kaspersky Security Center Cloud Console на свой компьютер или сервер. Kaspersky Security Center Cloud Console позволяет администратору устанавливать приложения безопасности "Лаборатории Касперского" на устройства в корпоративной сети, удаленно запускать задачи проверки и обновления, а также управлять политиками безопасности управляемых приложений. Администратор может использовать панель мониторинга, на которой показывается актуальное состояние корпоративных устройств, подробные отчеты и детальные параметры политик защиты.

Основные функции Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console позволяет сделать следующее:

- Устанавливать приложения "Лаборатории Касперского" на устройства вашей сети и управлять установленными приложениями.
- Формировать иерархию групп администрирования для управления набором клиентских устройств как единым целым.
- Создавать виртуальные Серверы администрирования и располагать их в иерархии.
- Защищать свои сетевые устройства, включая рабочие станции и серверы:
  - Управлять системой защиты, построенной на основе приложений "Лаборатории Касперского".
  - Использовать возможности обнаружения и реагирования (EDR и MDR) (требуется лицензия на Kaspersky Endpoint Detection and Response и/или на Kaspersky Managed Detection and Response), включая:
    - анализ и исследование инцидентов;
    - визуализацию инцидентов с помощью построения графика цепочки развития угроз;
    - принятие или отклонение ответов вручную или настройка автоматического принятия всех ответов.
- Kaspersky Security Center Cloud Console представляет собой мультитенантное приложение.

- Удаленно управлять установленными приложениями "Лаборатории Касперского" на клиентских устройствах.
- Централизованно распространять лицензионные ключи приложений "Лаборатории Касперского" на клиентские устройства.
- Создавать и контролировать политики безопасности для устройств в вашей сети.
- Создавать и контролировать учетные записи пользователей.
- Создавать и управлять ролями пользователей (RBAC).
- Создавать и контролировать задачи приложений, установленных на устройствах сети.
- Просматривать отчеты о состоянии системы защиты для каждой организации индивидуально.

О лицензировании Kaspersky Security Center Cloud Console для поставщиков услуг

Когда вы начинаете использовать Kaspersky Security Center Cloud Console, вы можете либо запросить пробную рабочую область (в этом случае вам предоставляется тридцатидневная пробная лицензия), либо ввести код активации для коммерческой лицензии.

Позже вы можете добавить один или несколько лицензионных ключей в хранилище Сервера администрирования.

О возможностях обнаружения и реагирования для поставщиков услуг

Kaspersky Security Center Cloud Console может интегрировать функции других приложений "Лаборатории Касперского" в интерфейсе консоли. Например, вы можете добавить функции обнаружения и реагирования к функциональности Kaspersky Security Center Cloud Console, интегрировав следующие приложения:

- Kaspersky Endpoint Detection and Response Optimum

  Kaspersky Endpoint Detection and Response Optimum – это решение, предназначенное для защиты ИТ-инфраструктуры организации от сложных киберугроз. Функциональность решения сочетает в себе автоматическое обнаружение угроз с возможностью реагирования на эти угрозы для защиты от сложных атак, включая новые эксплойты, приложения-шантажисты, бесфайловые атаки и методы, использующие законные системные инструменты.

  После того, как приложение "Лаборатории Касперского" Endpoint Protection Platform (EPP) обнаруживает инцидент безопасности, в Kaspersky Security Center Cloud Console создается подробная карточка с важными данными об инциденте безопасности. Карточка инцидента создается одним из следующих приложений:

  - Приложение Kaspersky Endpoint Agent, которое устанавливается вместе с приложением "Лаборатории Касперского", Endpoint Protection Platform (EPP).
  - Kaspersky Endpoint Security 11.7.0. для Windows и выше со встроенным функционалом EDR Optimum и не требует дополнительной установки Kaspersky Endpoint Agent.

Карточка инцидента позволяет анализировать и исследовать инцидент. Также вы можете визуализировать инцидент, создав график цепочки развития угроз. График описывает этапы развертывания обнаруженной атаки во времени. Созданный график включает информацию о модулях, участвующих в атаке, и действиях, выполняемых этими модулями.

Вы также можете инициировать цепочку ответных действий: создать правило предотвращения выполнения для ненадежного объекта; поиск похожих инцидентов в группе устройств по выбранным индикаторам взлома (IOC); изолировать ненадежный объект; изолировать взломанное устройство от сети.

Для получения информации об активации приложения см. документацию Kaspersky Endpoint Detection and Response Optimum.

Если интегрировано, это приложение добавляет раздел **Алерты** в интерфейс приложения Kaspersky Security Center Cloud Console (**Мониторинг** → **Алерты**).

- Kaspersky Managed Detection and Response

  Kaspersky Managed Detection and Response обеспечивает круглосуточную защиту от растущего объема угроз, которые обходят автоматические барьеры безопасности, организациям, которым сложно найти специалистов и персонал, или тем, у кого ограниченные внутренние ресурсы. Аналитики MDR SOC "Лаборатории Касперского" или сторонней компании исследуют инциденты и предлагают меры по их устранению. Вы можете принять или отклонить предложенные меры вручную или включить параметр автоматического принятия всех ответов.

  Информация об активации приложения приведена в документации Kaspersky Managed Detection and Response.

  Если интегрировано, это приложение добавляет раздел **Инциденты** в интерфейс приложения Kaspersky Security Center Cloud Console (**Мониторинг** → **Инциденты**).

Вы можете в любой момент показать или скрыть элементы интерфейса, относящиеся к функциям Kaspersky Endpoint Detection and Response или Kaspersky Managed Detection and Response в разделе **Параметры интерфейса** приложения Kaspersky Security Center Cloud Console.

Начало работы с Kaspersky Security Center Cloud Console

После выполнения сценария описанного в этом разделе, Kaspersky Security Center Cloud Console готов к использованию.

Сценарий начала работы

Сценарий состоит из следующих этапов:

1. **Создать учетную запись**

   Чтобы начать пользоваться Kaspersky Endpoint Security Cloud, необходима учетная запись Kaspersky Security Center Cloud Console.

Чтобы создать учетную запись:

1. Откройте браузер и введите следующий адрес: https://cloud.kaspersky.com.
2. Нажмите на кнопку **Создать учетную запись**.
3. Следуйте инструкциям на экране.

2. **Создать рабочую область**

   После создания учетной записи можно создать первую рабочую область. Рекомендуется сначала создать одну тестовую рабочую область, подключить к ней собственные устройства и протестировать изменение параметров, оценивая при этом результаты.

   Чтобы создать рабочую область:

   1. Откройте браузер и введите следующий адрес: https://cloud.kaspersky.com.
   2. Нажмите на кнопку **Войти**.
   3. Следуйте инструкциям на экране.

3. **Выполните первоначальную настройку Kaspersky Security Center Cloud Console**

   При первом входе в созданную рабочую область автоматически предлагается запустить мастер первоначальной настройки. Мастер первоначальной настройки позволяет создать минимальный набор необходимых задач и политик, настроить минимальный набор параметров и приступить к созданию инсталляционных пакетов приложений "Лаборатории Касперского". Следуйте инструкциям на экране.

После завершения начальной настройки приложение Kaspersky Security Center Cloud Console готово к использованию.

Рекомендации по управлению устройствами ваших клиентов

Этот раздел содержит рекомендации по организации клиентских устройств, которые вы хотите защитить.

Рекомендации зависят от того, используете ли вы приложение Kaspersky Security Center впервые или уже использовали локальную версию:

- Если вы никогда не использовали приложение Kaspersky Security Center ранее, у вас есть два варианта:
  - Создайте виртуальный Сервер администрирования для устройств каждого клиента (рекомендуемый вариант). В этом случае устройства каждого клиента могут управляться через выделенный виртуальный Сервер администрирования независимо от других клиентов. В то же время вы можете использовать главный Сервер администрирования для создания общих политик и задач для всех клиентов. Отчеты, формируемые на главном Сервере администрирования, могут включать данные со всех виртуальных Серверов администрирования.
  - Создайте группы администрирования устройств для каждого из клиентов. Если вы хотите дополнительно разделить клиентские устройства, вы можете создать иерархию подчиненных групп администрирования в каждой родительской группе. Например, вам могут понадобиться подчиненные группы, если вы хотите использовать разные параметры защиты для устройств сотрудников, работающих в разных отделах.

- Если вы уже использовали Kaspersky Security Center, работающий локально, вы можете перенести существующие группы администрирования и связанные объекты из локального Kaspersky Security Center в Kaspersky Security Center Cloud Console.

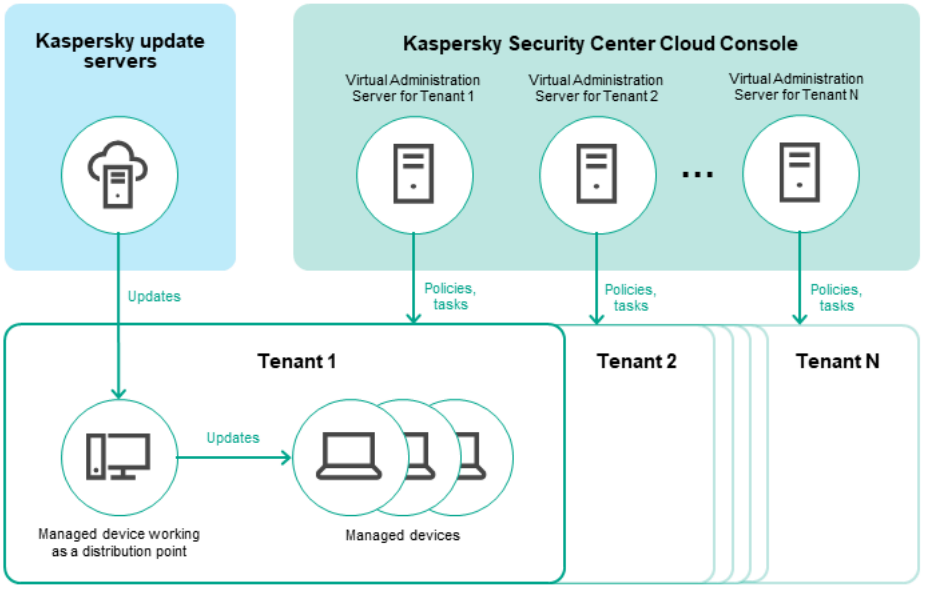
  Вы не можете перенести виртуальные Серверы администрирования. После переноса групп администрирования и других объектов вы можете создавать виртуальные Серверы администрирования в Kaspersky Security Center Cloud Console.

  Перейдите к настройке переноса данных.

Администратор виртуального Сервера администрирования может перейти на этот виртуальный Сервер только с главного Сервера администрирования. Все объекты, созданные на главном Сервере администрирования, доступны для чтения администратору виртуального Сервера администрирования (например, виджеты, отчеты или роли пользователей).

Типовые способы развертывания системы защиты для поставщиков услуг

В этом разделе представлено описание схемы развертывания, обычно используемой поставщиками услуг для управления несколькими тенантами. Схема основана на управлении с помощью виртуальных Серверов администрирования, индивидуально созданных для каждого тенанта.



Типовые способы развертывания системы защиты для поставщиков услуг

Схема состоит из следующих основных компонентов:

- *Kaspersky Security Center Cloud Console*. Приложение предоставляет пользовательский интерфейс для служб администрирования вашего рабочего места. Вы используете Kaspersky Security Center Cloud Console для развертывания, управления и обслуживания системы защиты сети организации-клиента.

- *Серверы обновлений "Лаборатории Касперского"*. HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложений.

- *Виртуальные Серверы администрирования*. Администратор поставщика услуг обычно создает виртуальный Сервер администрирования для каждого тенанта для развертывания, управления и обслуживания системы защиты сети соответствующей клиентской организации.

- *Тенанты*. Клиентские организации, чьи устройства должны быть защищены.

- *Управляемые устройства*. Клиентские устройства организации защищены Kaspersky Security Center Cloud Console. На каждом защищаемом устройстве должны быть установлены Агент администрирования и одно из приложений безопасности "Лаборатории Касперского".

- *Управляемое устройство, выполняющее роль точки распространения*. Устройство с установленным Агентом администрирования, которое используется для распространения обновлений, опроса сети, удаленной установки приложений, получения информации об устройствах в составе группы администрирования и/или широковещательного домена. Администратор выбирает соответствующие устройства и вручную назначает их точками распространения. Точки распространения также могут выступать в качестве шлюзов соединения для уменьшения количества исходящих внешних подключений и количества одновременных подключений к Серверу администрирования. Рекомендуется ограничить количество управляемых устройств, которые напрямую подключены к Серверу администрирования.

Сценарий: развертывание защиты (управление тенантами с помощью виртуальных Серверов администрирования)

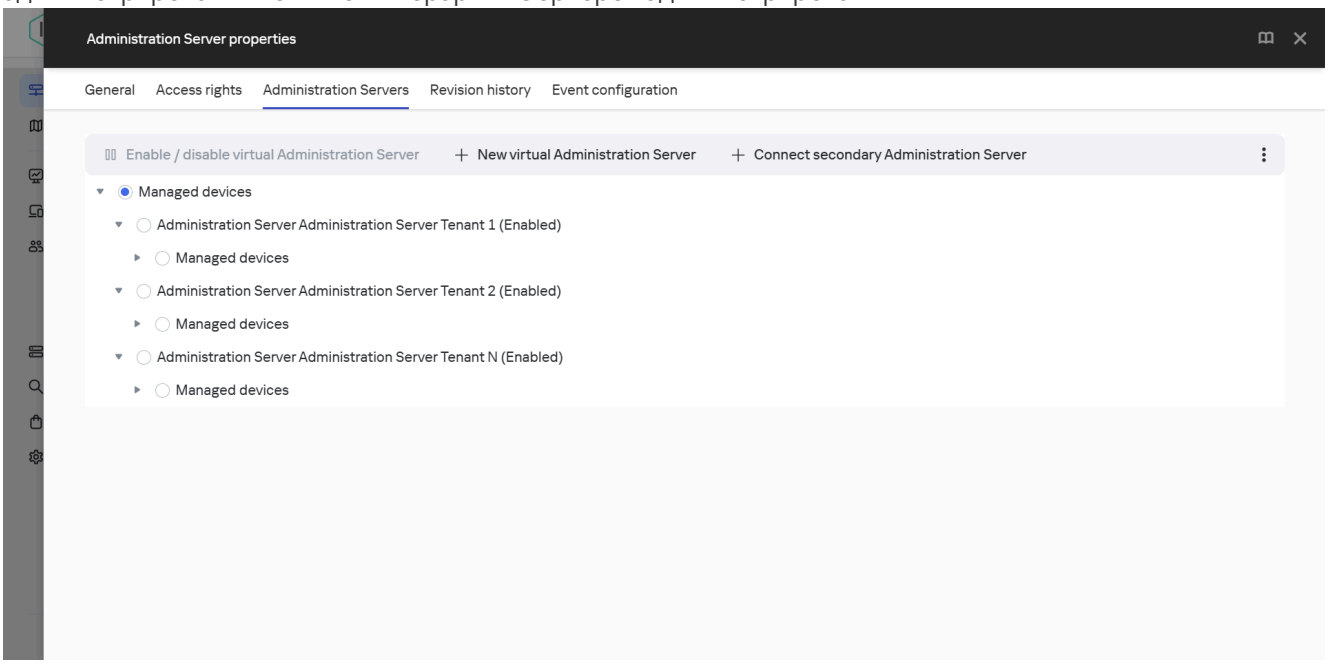
Если вы никогда не использовали Kaspersky Security Center и хотите управлять своими тенантами с помощью виртуальных Серверов администрирования, действуйте, как описано в этом разделе. После завершения этого сценария устройства ваших клиентов будут защищены.

Если вы управляете несколькими тенантами, то выполняйте сценарий для каждого из тенантов отдельно.

Сценарий состоит из следующих этапов:

1. **Создание виртуального Сервера администрирования**

   Создайте виртуальный Сервер администрирования для вашего клиента. Новый виртуальный Сервер администрирования появится в иерархии Серверов администрирования:



Виртуальные Серверы администрирования в иерархии Серверов администрирования

2. **Выбор устройств, которые выполняют роль точек распространения**

   Принятие решения о том, какое именно из устройств будет выполнять роль точки распространения.

   > В одной рабочей области не может быть более 100 точек распространения.

3. **Создание автономного инсталляционного пакета Агента администрирования**

   Переключитесь на созданный виртуальный Сервер администрирования, а затем создайте автономный инсталляционный пакет для Агента администрирования. Вы можете переключать Серверы администрирования в главном меню, нажав на значок шеврона (›) справа от имени текущего Сервера администрирования и выбрав требуемый Сервер администрирования. При создании автономного инсталляционного пакета укажите группу администрирования Управляемые устройства, в которую нужно переместить устройство.

4. **Установка Агента администрирования на выбранное устройство, выполняющее роль точки распространения**

   Вы можете использовать любой способ, который подходит вам:

   - Ручная установка

     Чтобы доставить автономный инсталляционный пакет на устройство, вы можете, например, скопировать его на съемный диск (например, флеш-накопители) или поместить в общую папку.

   - Развертывание с использованием Active Directory

   - Развертывание с использованием решения для удаленного мониторинга и управления (RMM).

5. **Назначение точки распространения**

   Назначьте устройства с установленным Агентом администрирования точкой распространения.

6. **Опрос сети**

   Настройка и выполнение опроса сети точками распространения.

   Kaspersky Security Center Cloud Console предоставляет следующие способы опроса сети:

   - Опрос IP-диапазонов

   - Опрос сети Windows

   - Опрос Active Directory

   После завершения опроса сети в соответствии с расписанием устройства ваших клиентов обнаруживаются и помещаются в группу **Нераспределенные устройства**.

7. **Перемещение обнаруженных устройств в группы администрирования**

   Настройте правила автоматического перемещения обнаруженных устройств в требуемые группы администрирования; или переместите эти устройства в требуемые группы администрирования вручную. Если вы планируете управлять устройствами клиента в одной группе администрирования, вы можете переместить устройства в группу Управляемые устройства.

8. **Создание инсталляционных пакетов для Агента администрирования и управляемых программ "Лаборатории Касперского"**

   Создание инсталляционных пакетов для приложений "Лаборатории Касперского".

9. **Удаление приложений безопасности сторонних производителей**

   Если на устройствах клиентов установлены приложения безопасности сторонних производителей, удалите их перед установкой приложений "Лаборатории Касперского".

10. **Установка программ "Лаборатории Касперского" на клиентские устройства**

    Создание задач удаленной установки приложений для установки Агента администрирования и управляемых приложений "Лаборатории Касперского" на устройства ваших клиентов.

    При необходимости вы можете создать несколько задач удаленной установки, чтобы установить управляемые приложения "Лаборатории Касперского" для различных групп администрирования или выборок устройств.

    После создания задач, вы можете настроить их параметры. Убедитесь, что расписание запуска каждой задачи соответствует вашим требованиям. Сначала должна быть запущена задача установки Агента администрирования. После установки Агента администрирования на устройства клиентов необходимо запустить задачу установки управляемых приложений "Лаборатории Касперского".

11. **Проверка первоначального развертывания приложений "Лаборатории Касперского"**

    Сформируйте и просмотрите **Отчет о версиях приложений "Лаборатории Касперского"**. Убедитесь, что управляемые приложения "Лаборатории Касперского" установлены на всех устройствах клиента.

12. **Создание политик для приложений "Лаборатории Касперского"**

    Создайте политику для требуемой программы "Лаборатории Касперского". Если вы хотите создать универсальную политику для всех своих клиентов, переключите текущий виртуальный Сервер администрирования на главный Сервер администрирования, а затем создайте политику для нужного приложения "Лаборатории Касперского".

Сценарий: развертывание защиты (управление с помощью групп администрирования)

Если вы никогда не использовали Kaspersky Security Center и хотите управлять тенантами с помощью групп администрирования, действуйте, как описано в этом разделе. После завершения этого сценария устройства ваших клиентов будут защищены.

Сценарий состоит из следующих этапов:

1. **Создание групп администрирования**

   Создание группы администрирования для каждого из ваших клиентов.

2. **Планирование структуры точек распространения**

   Принятие решения о том, какое именно из устройств каждого будет выполнять роль точки распространения.

   > В одной рабочей области не может быть более 100 точек распространения.

3. **Создание автономного инсталляционного пакета Агента администрирования**

   Создайте автономный инсталляционный пакет Агента администрирования.

4. **Установка Агента администрирования на выбранные устройства, выполняющие роль точек распространения**

Установка Агента администрирования на выбранные устройства, выполняющие роль точек распространения.

Вы можете использовать любой способ, который подходит вам:

- Ручная установка

  Чтобы доставить автономный инсталляционный пакет на устройства, вы можете, например, скопировать его на съемный диск (например, флеш-накопители) или поместить в общую папку.

- Развертывание с использованием Active Directory

- Развертывание с использованием решения для удаленного мониторинга и управления (RMM).

5. **Назначение точек распространения**

   Назначьте устройства с установленным Агентом администрирования точками распространения.

6. **Опрос сети**

   Настройка и выполнение опроса сети точками распространения.

   Kaspersky Security Center Cloud Console предоставляет следующие способы опроса сети:

   - Опрос IP-диапазонов
   - Опрос сети Windows
   - Опрос Active Directory

   После завершения опроса сети в соответствии с расписанием устройства ваших клиентов обнаруживаются и помещаются в группу **Нераспределенные устройства**.

7. **Перемещение обнаруженных устройств в группы администрирования**

   Настройте правила автоматического перемещения обнаруженных устройств в требуемые группы администрирования; или переместите эти устройства в требуемые группы администрирования вручную.

8. **Создание инсталляционных пакетов для Агента администрирования и управляемых приложений "Лаборатории Касперского"**

   Если вы не запускали мастер первоначальной настройки или пропустили этап создания инсталляционных пакетов, создайте инсталляционные пакеты для приложений "Лаборатории Касперского".

9. **Удаление приложений безопасности сторонних производителей**

   Если на устройствах клиентов установлены приложения безопасности сторонних производителей, удалите их перед установкой приложений "Лаборатории Касперского".

10. **Установка приложений "Лаборатории Касперского" на устройства клиентов**

    Создание задач удаленной установки приложений для установки Агента администрирования и управляемых приложений "Лаборатории Касперского" на устройства ваших клиентов.

    При необходимости вы можете создать несколько задач удаленной установки, чтобы установить управляемые приложения "Лаборатории Касперского" для различных групп администрирования или выборок устройств.

    После создания задач, вы можете настроить их параметры. Убедитесь, что расписание запуска каждой задачи соответствует вашим требованиям. Сначала должна быть запущена задача установки Агента администрирования. После установки Агента администрирования на устройства клиентов необходимо запустить задачу установки управляемых приложений "Лаборатории Касперского".

11. **Проверка первоначального развертывания приложений "Лаборатории Касперского"**

    Сформируйте и просмотрите **Отчет о версиях приложений "Лаборатории Касперского"**. Убедитесь, что управляемые приложения "Лаборатории Касперского" установлены на всех устройствах клиентов.

12. **Создание политик для приложений "Лаборатории Касперского"**

    Перейдите в раздел **Управление активами** → **Группы**. Если вы хотите создать универсальную политику для всех клиентов, выберите **Сервер администрирования.** Если вы хотите создать определенную политику для определенного клиента, выберите группу администрирования, соответствующую этому клиенту. Создайте политику для требуемого приложения "Лаборатории Касперского".

Совместное использование приложения Kaspersky Security Center, работающего локально, и Kaspersky Security Center Cloud Console

Если вы уже использовали Kaspersky Security Center, работающий локально, вы можете преобразовать существующие Серверы администрирования, работающие локально, в подчиненные Серверы администрирования вашего нового Сервера администрирования Kaspersky Security Center Cloud Console, как описано в этом разделе.

Если вы настроите совместное использование приложения Kaspersky Security Center, работающего локально, и Kaspersky Security Center Cloud Console, вы не сможете перенести данные из приложения Kaspersky Security Center, работающего локально, в Kaspersky Security Center Cloud Console, пока не удалите иерархию Серверов администрирования.

Чтобы создать иерархию Серверов администрирования,

добавьте существующие Серверы администрирования, работающие локально, в качестве подчиненных Серверов администрирования.

Лицензирование приложений "Лаборатории Касперского" для поставщиков услуг

Kaspersky Security Center Cloud Console позволяет централизованно распространять лицензионные ключи приложений "Лаборатории Касперского" на устройства клиентов, наблюдать за использованием ключей и продлевать сроки действия лицензий.

Если вы управляете несколькими тенантами, вы можете распространять лицензионные ключи следующими способами:

- Один лицензионный ключ для всех тенантов.
- Индивидуальный лицензионный ключ для каждого тенанта.

Чтобы распространить лицензионные ключи на устройства ваших клиентов:

1. Добавьте требуемые лицензионные ключи в хранилище Сервера администрирования.
2. Выполните одно из следующих действий:
   - Настройте автоматическое распространение лицензионного ключа.

     В этом случае Kaspersky Security Center Cloud Console выбирает один из применимых лицензионных ключей и автоматически распространяет его при каждом обнаружении нового устройства.
   - Настройте задачу Добавить лицензионный ключ для распространения лицензионного ключа на устройства.

     При настройке задачи вы выбираете лицензионный ключ, который должен быть распространен на устройства, и выбираете группу администрирования, которая содержит необходимые устройства.

     Одна задача может распространять только один лицензионный ключ. Если вы хотите распространять несколько лицензионных ключей, вам нужно создать задачу для каждого из них.

Приложения "Лаборатории Касперского", установленные на устройствах ваших клиентов, активированы.

Добавление активного лицензионного ключа на главный Сервер администрирования обязательно. Иначе связанная рабочая область будет удалена через 90 дней, независимо от статуса лицензионных ключей на других Серверах администрирования в этой рабочей области.

Функции мониторинга и работа с отчетами для поставщиков услуг

Kaspersky Security Center Cloud Console предоставляет вам возможности мониторинга и работы с отчетами. Эти функции позволяют получать сведения об инфраструктуре вашей организации и статусах защиты, а также статистику.

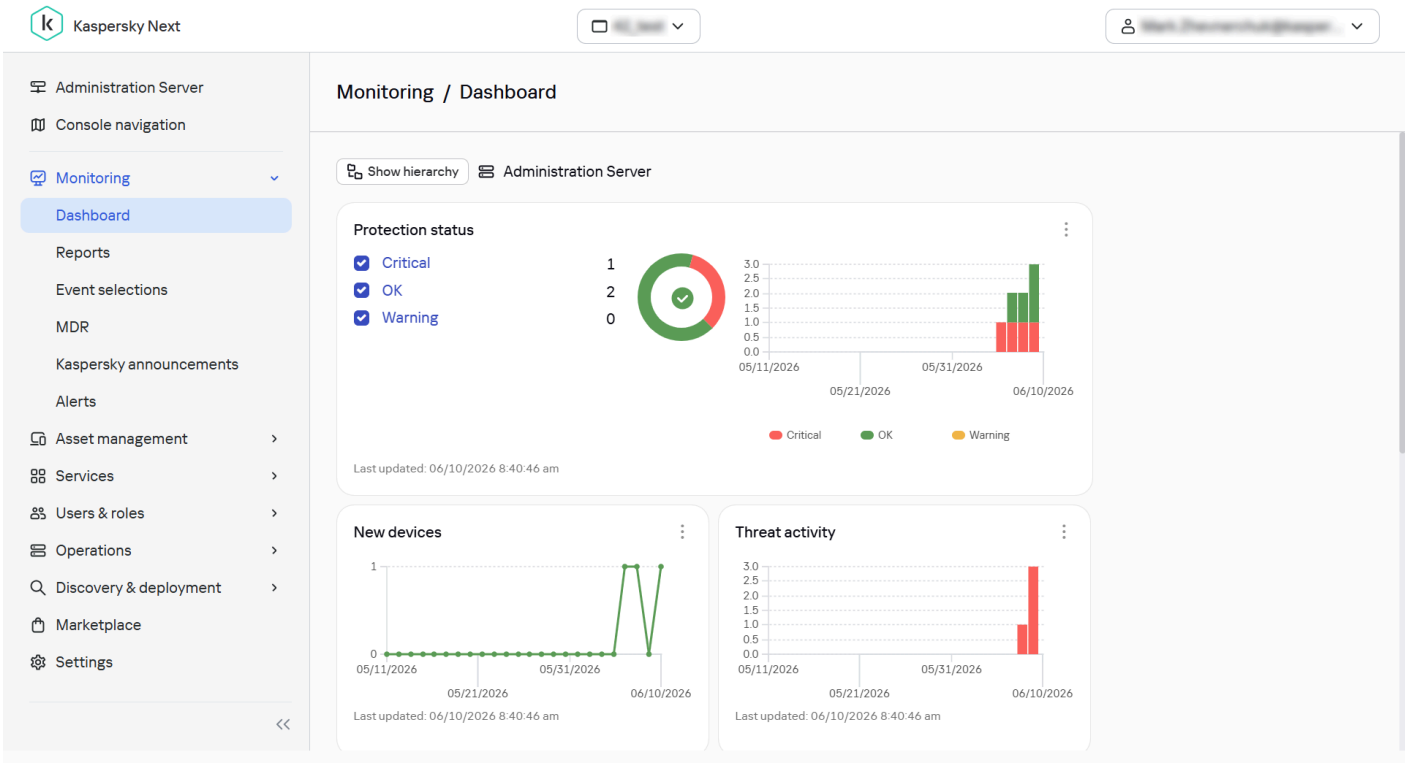
После развертывания Kaspersky Security Center Cloud Console вы можете настроить функции мониторинга и отчетности.

Kaspersky Security Center Cloud Console предоставляет следующие типы мониторинга и работы с отчетами:

- Панель мониторинга
- Отчеты
- Выборки событий
- Уведомления по электронной почте

Панель мониторинга

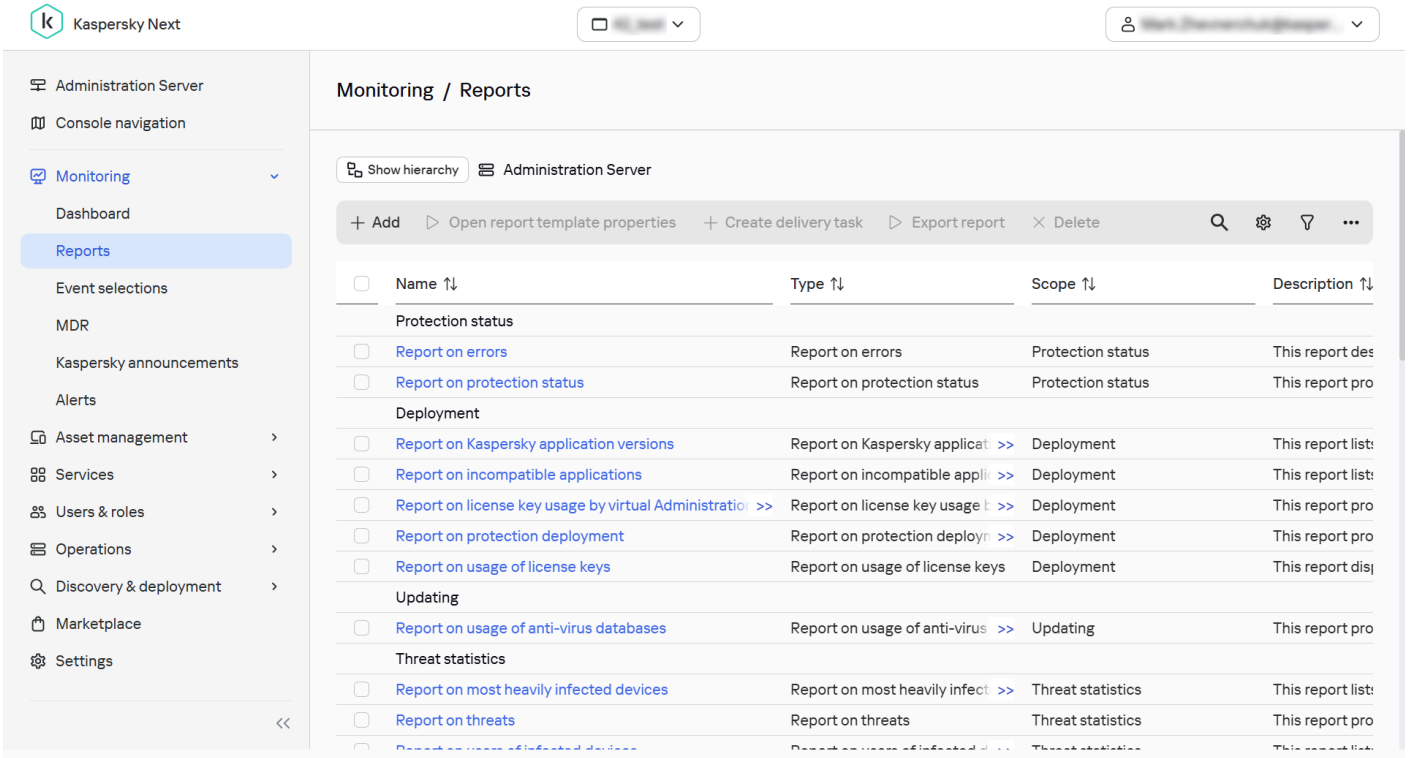
Панель мониторинга позволяет контролировать состояние безопасности в сети вашей организации с помощью графического представления информации. (См. рисунок ниже.)



Раздел "Панель мониторинга"

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. Вы можете настроить расписание отправки отчетов по электронной почте (см. рисунок ниже).



Раздел "Отчеты"

Выборки событий

Выборки событий позволяют просматривать на экране именованные наборы событий, выбранные из базы данных Сервера администрирования. Kaspersky Security Center Cloud Console содержит ряд предопределенных выборок событий (например, **Последние события** и **Критические события**). Вы также можете создавать собственные выборки событий.

Уведомления по электронной почте.

Вы можете настроить уведомления по электронной почте о событиях, возникающих в Kaspersky Security Center Cloud Console и на устройствах ваших клиентов.

Работа с Kaspersky Security Center Cloud Console в облачном окружении

В этом разделе представлена информация о функциях Kaspersky Security Center Cloud Console, связанных с эксплуатацией и обслуживанием Kaspersky Security Center Cloud Console в облачных окружениях, таких как Amazon Web Services, Microsoft Azure и Google Cloud.

Для работы в облачном окружении вам нужна специальная лицензия. Если у вас нет такой лицензии, элементы интерфейса, связанные с облачными устройствами, не работают.

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

Варианты лицензирования в облачном окружении

Работа в облачном окружении возможна как в пробном, так и в коммерческом режиме Kaspersky Security Center Cloud Console:

- В пробном режиме все функции облачного окружения доступны в течение всего срока действия вашей рабочей области. Лицензия не требуется.
- В коммерческом режиме возможности облачного окружения доступны только в том случае, если лицензионный ключ Kaspersky Security для виртуальных и облачных сред добавлен как активный в свойствах Сервера администрирования.

В обоих случаях автоматически активируется Системное администрирование.

Если возникает ошибка при попытке активировать функцию Поддержка облачного окружения с использованием лицензии Kaspersky Security для виртуальных и облачных сред, используйте файл ключа.

Подготовка к работе в облачном окружении с помощью Kaspersky Security Center Cloud Console

В этом разделе описано, как подготовиться к работе с Kaspersky Security Center Cloud Console в следующих облачных окружениях:

- Amazon Web Services;
- Microsoft Azure;
- Google Cloud.

Работа в облачном окружении Amazon Web Services

В этом разделе описано, как подготовиться к работе с Kaspersky Security Center Cloud Console в Amazon Web Services.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky Security Center Cloud Console.

О работе в облачном окружении Amazon Web Services

Для работы с платформой AWS, и в частности для того, чтобы создавать инстансы, вам потребуется учетная запись в Amazon Web Services. Вы можете создать бесплатную учетную запись на сайте https://aws.amazon.com/ru. Вы также можете использовать существующую учетную запись Amazon.

О том, что такое образы AMI и как работает магазин приложений AWS Marketplace, см. на странице справки AWS Marketplace. О работе с платформой AWS, об использовании инстансов и о связанных с ними понятиях см. в документации Amazon Web Services.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky Security Center Cloud Console.

Создание учетных записей IAM-пользователя для инстансов Amazon EC2

В этом разделе описано, какие действия необходимо выполнить, чтобы обеспечить корректную работу Kaspersky Security Center Cloud Console. Эти действия включают работу с сервисами AWS с учетными записям IAM-пользователей (Identity and Access Management). Также описано, какие действия должны быть выполнены с клиентскими устройствами, чтобы установить на них Агент администрирования и затем защитные приложения Kaspersky Endpoint Security для Linux.

Обеспечение прав для работы Kaspersky Security Center Cloud Console с AWS

Для работы в облачном окружении Amazon Web Services с помощью Kaspersky Security Center Cloud Console необходимо создать *учетную запись IAM-пользователя*, которую Kaspersky Security Center Cloud Console будет использовать для работы с сервисами AWS. Прежде чем начинать работу с Сервером администрирования, создайте учетную запись IAM-пользователя с *ключом доступа AWS IAM* (далее также *ключ доступа IAM*).

Для создания IAM-пользователя требуется Консоль управления AWS. Для работы с Консолью управления AWS вам понадобятся имя пользователя и пароль от учетной записи в AWS.

Создание учетной записи IAM-пользователя для работы Kaspersky Security Center Cloud Console

Учетная запись IAM-пользователя необходима для работы с Kaspersky Security Center Cloud Console. Вы можете создать одну учетную запись IAM-пользователя с требуемыми правами или две разные учетные записи.

Для IAM-пользователя автоматически создается *ключ доступа IAM*, который вам потребуется предоставить Kaspersky Security Center Cloud Console на этапе первоначальной настройки. Ключ доступа IAM состоит из ID ключа доступа и секретного ключа. Подробнее о службе IAM см. на следующих справочных страницах AWS:

- https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.
- https://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

Чтобы создать учетную запись IAM-пользователя с необходимыми правами:

1. Откройте Консоль управления AWS и войдите под своей учетной записью.
2. В списке служб AWS выберите **IAM**.

   Откроется окно, содержащее список имен пользователей и меню, с помощью которого вы сможете работать с инструментом.
3. Перейдите к областям консоли, использующим учетные записи пользователей, и добавьте новое имя пользователя или имена.
4. Для пользователей, которых вы добавили, укажите следующие параметры AWS:
   - Тип доступа: **Programmatic Access**.
   - Границы разрешений не установлены.
   - Разрешение: **ReadOnlyAccess**.

     После добавления разрешения просмотрите его на предмет точности. В случае ошибки выбора параметров перейдите к предыдущему экрану и выполните выбор параметров снова.
5. После того как вы создали учетную запись, отобразится таблица с ключом доступа IAM нового IAM-пользователя. ID ключа доступа отобразится в столбце **Access key ID**. Секретный ключ отобразится в столбце **Secret access key** в виде звездочек. Чтобы посмотреть секретный ключ, нажмите **Show**.

Созданная учетная запись отобразится в списке учетных записей IAM-пользователей, соответствующих вашей учетной записи в AWS.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky Security Center Cloud Console.

Работа в облачном окружении Microsoft Azure

В этом разделе представлена информация о том, как работать с Kaspersky Security Center Cloud Console в облачном окружении, предоставленном платформой Microsoft Azure, и как развернуть защиту на виртуальных машинах внутри облачного окружения.

О работе в Microsoft Azure

Чтобы работать с платформой Microsoft Azure, в частности для покупки приложений в магазине Azure Marketplace и создания виртуальных машин, вам потребуется подписка Azure. Перед тем как начать работу с Microsoft Azure в Kaspersky Security Center Cloud Console, создайте ID приложения в Azure с правами, необходимыми для установки приложения на виртуальные машины.

Создание подписки, идентификатора приложения и пароля

Для работы с Kaspersky Security Center Cloud Console в окружении Microsoft Azure вам нужны подписка Azure, ID приложения в Azure и пароль приложения в Azure. Вы можете использовать существующую подписку, если у вас она уже есть.

Подписка Azure предоставляет владельцу доступ к Microsoft Azure Platform Management Portal и сервисам Microsoft Azure. Владелец может использовать Microsoft Azure Platform, чтобы управлять службами, такими как Azure SQL и Azure Storage.

Чтобы создать подписку Microsoft Azure,

Перейдите по ссылке https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/create-subscription и следуйте инструкциям.

Подробная информация о создании подписки доступна на сайте Microsoft. Вы получите идентификатор подписки, который затем предоставите Kaspersky Security Center Cloud Console вместе с ID приложения и паролем.

Чтобы создать и сохранить ID приложения и пароль Azure:

1. Перейдите по ссылке https://portal.azure.com и убедитесь, что выполнен вход.
2. Следуя инструкциям на странице справки, создайте ID приложения.
3. В свойствах приложения перейдите в раздел **Keys**.
4. В разделе **Keys** заполните поля **Description** и **Expires** и оставьте поле **Value** пустым.
5. Нажмите на кнопку **Сохранить**.

   После того как вы нажмете на кнопку **Save**, система автоматически заполнит поле **Value** длинной последовательностью символов. Эта последовательность символов является вашим паролем приложения в Azure (например, yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU=). Описание отображается так, как вы его указали.

6. Скопируйте пароль и сохраните его, чтобы позже вы смогли предоставить ID приложения и пароль в Kaspersky Security Center Cloud Console.

   Вы можете скопировать пароль только при его создании. Позже пароль больше не будет отображаться, и вы не сможете его восстановить.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky Security Center Cloud Console.

Назначение роли для ID приложения в Azure

Если требуется только обнаружить виртуальные машины с помощью процесса обнаружения устройств, ID приложения в Azure должна быть назначена роль Читатель (Reader). Если требуется не только обнаружить виртуальные машины, но и развернуть защиту с помощью Azure API, ваш ID приложения в Azure должен иметь роль Участник виртуальных машин (Virtual Machine Contributor).

Следуйте инструкциям, приведенным на веб-сайте Microsoft, чтобы назначить роль для ID приложения в Azure.

Работа в Google Cloud

Этот раздел содержит информацию о работе с Kaspersky Security Center Cloud Console в облачном окружении, предоставляемом Google.

API Google можно использовать для работы с Kaspersky Security Center Cloud Console на платформе Google Cloud. Требуется учетная запись Google. Дополнительную информацию вы можете найти в документации Google на странице https://cloud.google.com.

Вам нужно создать и предоставить Kaspersky Security Center Cloud Console следующие учетные данные:

- **Электронная почта клиента**

  Электронная почта клиента – это адрес электронной почты, который вы использовали для регистрации вашего проекта в Google Cloud.

- **Идентификатор проекта.**

  Идентификатор проекта – это идентификатор, полученный при регистрации проекта Google Cloud.

- **Закрытый ключ.**

  Закрытый ключ – это последовательность символов, которые вы получили в качестве закрытого ключа при регистрации проекта в Google Cloud. Вы можете скопировать и вставить эту последовательность, чтобы избежать ошибок.

Мастер настройки для работы в облачном окружении в Kaspersky Security Center Cloud Console

Для настройки Kaspersky Security Center Cloud Console с помощью этого мастера вам потребуется следующее:

- Укажите учетные данные для облачного окружения:
  - учетная запись IAM-пользователя, которому предоставлено право опроса облачного сегмента (для работы с Amazon Web Services);
  - идентификатор приложения в Azure, пароль и подписка (для работы с Microsoft Azure);
  - электронная почта клиента Google, идентификатор проекта и закрытый ключ (для работы с Google Cloud).
- Инсталляционные пакеты:
  - Агент администрирования для Windows
  - Агент администрирования для Linux
  - Kaspersky Endpoint Security для Linux
- Веб-плагин Kaspersky Endpoint Security для Linux.
- Хотя бы одно из следующего:
  - инсталляционный пакет и веб-плагин Kaspersky Endpoint Security для Windows (рекомендуется);
  - инсталляционный пакет и веб-плагин Kaspersky Security для Windows Server или Linux Server.

Если ваша рабочая область была создана с использованием лицензии Kaspersky Security для виртуальных и облачных сред, мастер настройки облачного окружения запускается автоматически при первом подключении к Kaspersky Security Center Cloud Console. Если вы пропустите мастер настройки облачного окружения, он будет запускаться при каждом подключении к Kaspersky Security Center Cloud Console, пока вы не выполните все шаги мастера.

Вы также можете запустить мастер настройки для работы в облачном окружении вручную в любое время.

Чтобы запустить мастер настройки для работы в облачном окружении вручную:

В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Настройка работы в облачном окружении**.

Запустится мастер настройки для работы в облачном окружении.

Приблизительное время работы с мастером составляет около пятнадцати минут.

Если вы не активировали Сервер администрирования по лицензии Kaspersky Security для виртуальных и облачных сред, вам нужно выполнить это на первом шаге мастера.

Шаг 1. Проверка требуемых плагинов и инсталляционных пакетов

Этот шаг не отображается, если у вас есть все необходимые веб-плагины и инсталляционные пакеты, перечисленные ниже.

Для настройки облачного окружения требуется наличие следующих компонентов:

- Инсталляционные пакеты:
  - Агент администрирования для Windows
  - Агент администрирования для Linux
  - Kaspersky Endpoint Security для Linux
- Веб-плагин Kaspersky Endpoint Security для Linux.
- Инсталляционный пакет и веб-плагин Kaspersky Endpoint Security для Windows.

Kaspersky Security Center Cloud Console автоматически определяет уже имеющиеся компоненты и перечисляет только те, которых не хватает. Загрузите перечисленные компоненты, нажав на кнопку **Выберите приложения для загрузки**, и выберите необходимые плагины и инсталляционные пакеты. После загрузки компонента вы можете использовать кнопку **Обновить**, чтобы обновить список отсутствующих компонентов.

Шаг 2. Выбор способа активации приложения

Этот шаг отображается, только если при создании рабочей области вы использовали лицензию, отличную от Kaspersky Security для виртуальных и облачных сред, и никогда не добавляли лицензионный ключ Kaspersky Security для виртуальных и облачных сред в поле активации Сервера администрирования. В этом случае вам необходимо активировать Сервер администрирования с использованием лицензии Kaspersky Security для виртуальных и облачных сред.

Шаг 3. Выбор облачного окружения и аутентификация

Задайте следующие параметры:

- **Облачное окружение**

  Выберите облачное окружение, в котором вы разворачиваете Kaspersky Security Center Cloud Console: AWS, Azure или Google Cloud.

  Если вы планируете работать с несколькими облачными окружениями, выберите одно облачное окружение и потом запустите мастер еще раз.

- **Название соединения**

  Введите имя для соединения. Название может содержать не более 256 символов. Допустимы только символы Юникод.

  Это имя будет также использоваться как имя группы администрирования для облачных устройств.

  Если вы планируете работать с несколькими облачными окружениями, возможно, вы захотите включить имя среды в название соединения, например, "Сегмент Azure", "Сегмент AWS" или "Сегмент Google".

Введите свои учетные данные, чтобы получить аутентификацию в облачном окружении, которое вы указали.

AWS

Если вы выбрали AWS в качестве типа облачного сегмента, используйте ключ доступа AWS IAM для дальнейшего опроса облачного сегмента. Введите следующие данные ключа:

- **ID ключа доступа**

  ID ключа доступа IAM – это последовательность из букв и цифр. Вы получили ID ключа при создании учетной записи IAM-пользователя.

  Поле доступно, если вы выбрали для авторизации ключ доступа AWS IAM.

- **Секретный ключ**

  Секретный ключ, который вы получили с ID ключа доступа при создании учетной записи IAM-пользователя.

  Символы секретного ключа отображаются в виде звездочек. После того, как вы начали вводить секретный ключ, отображается кнопка **Показать**. Нажмите на эту кнопку и удерживайте ее необходимое вам время, чтобы просмотреть введенные символы.

  Поле доступно, если вы выбрали для авторизации ключ доступа AWS IAM.

  Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

Azure

Если вы выбрали Azure в качестве типа облачного сегмента, укажите следующие параметры соединения, которые в дальнейшем будут использоваться для опроса облачного сегмента:

- **Идентификатор приложения в Azure**

  Вы создали этот идентификатор приложения на портале Azure.

Вы можете указать только один идентификатор приложения в Azure для опроса и других целей. Если необходимо опрашивать другой сегмент Azure, вам нужно сначала удалить первый сегмент в существующем соединении Azure.

- **Идентификатор подписки Azure**

  Вы создали подписку на портале Azure.

- **Пароль приложения Azure**

  Вы получили пароль к идентификатору приложения при создании ID приложения в Azure.

  Символы пароля отображаются в виде звездочек. После того, как вы начали вводить пароль, отображается кнопка **Показать**. Нажмите и удерживайте эту кнопку, чтобы просмотреть введенные символы.

  Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

- **Имя учетной записи хранения Azure**

  Вы создали имя учетной записи хранения Azure для работы с Kaspersky Security Center Cloud Console.

- **Ключ доступа хранилища Azure**

  Вы получили пароль (ключ) при создании учетной записи хранения Azure для работы с Kaspersky Security Center Cloud Console.

  Ключ доступен в разделе "Overview of the Azure storage account" в подразделе "Keys".

  Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

Google Cloud

Если вы выбрали Google Cloud в качестве типа облачного сегмента, укажите следующие параметры соединения, которые в дальнейшем будут использоваться для опроса облачного сегмента:

- **Электронная почта клиента**

  Электронная почта клиента – это адрес электронной почты, который вы использовали для регистрации вашего проекта в Google Cloud.

- **ID проекта**

  Идентификатор проекта – это идентификатор, полученный при регистрации проекта Google Cloud.

- **Закрытый ключ**

  Закрытый ключ – это последовательность символов, которые вы получили в качестве закрытого ключа при регистрации проекта в Google Cloud. Вы можете скопировать и вставить эту последовательность, чтобы избежать ошибок.

  Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

Указанное соединение сохранится в параметрах приложения.

Мастер настройки для работы в облачном окружении дает возможность указать только один сегмент. В дальнейшем вы можете указывать и другие соединения для управления другими облачными сегментами.

Нажмите на кнопку **Далее**, чтобы продолжить.

Шаг 4. Опрос сегментов и настройка синхронизации с облачным окружением

На этом шаге начинается опрос облачного сегмента и автоматически создается специальная группа администрирования для облачных устройств. Устройства, обнаруженные при опросе, перемещаются в эту группу. Расписание опроса облачного сегмента настроено (по умолчанию каждые пять минут; вы можете изменить этот параметр позже).

Также создается правило автоматического перемещения **Синхронизация с облачным окружением**. При каждом последующем сканировании облачной сети обнаруженные виртуальные устройства будут перемещаться в соответствующую подгруппу внутри группы **Управляемые устройства****Cloud**.

Укажите параметр **Синхронизировать группы администрирования с облачной структурой**.

Если параметр включен, то в группе **Управляемые устройства** автоматически создается группа **Cloud** и запускается процесс обнаружения устройств в облачной сети. Инстансы и виртуальные машины, обнаруженные во время каждого сканирования облачной сети, перемещаются в группу Cloud. Структура подгрупп администрирования в этой группе соответствует структуре вашего облачного сегмента (в AWS зоны доступности и группы размещения не представлены в структуре; в Azure подсети не представлены в структуре). Устройства, не идентифицированные как инстансы в облачном окружении, находятся в группе **Нераспределенные устройства**. Такая структура групп позволяет устанавливать антивирусные приложения на инстансы с помощью задач групповой установки и настраивать разные политики для разных групп.

Если параметр выключен, то также создается группа **Cloud** и запускается процесс обнаружения устройств в облачной сети, однако в группе не создаются подгруппы, соответствующие структуре облачного сегмента. Все найденные инстансы находятся в группе администрирования **Cloud** и отображаются единым списком. Если в процессе работы с Kaspersky Security Center Cloud Console вам потребуется произвести синхронизацию, то вы сможете изменить свойства правила **Синхронизация с облачным окружением** и форсировать его. Применение правила перестраивает структуру групп внутри группы Cloud так, чтобы она соответствовала структуре вашего облачного сегмента.

По умолчанию параметр выключен.

Нажмите на кнопку **Далее**, чтобы продолжить.

Шаг 5. Настройка Kaspersky Security Network для Kaspersky Security Center Cloud Console

Этот шаг пропускается при запуске Kaspersky Security Center Cloud Console в пробном режиме или на виртуальном Сервере администрирования.

Настройте параметры передачи информации о работе Kaspersky Security Center Cloud Console в базу знаний Kaspersky Security Network (KSN). Выберите один из следующих вариантов:

- **Я принимаю условия использования Kaspersky Security Network**

  Kaspersky Security Center Cloud Console 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 Cloud Console и управляемые приложения не будут предоставлять информацию о своей работе Kaspersky Security Network.

  Если вы выбрали этот параметр, использование Kaspersky Security Network будет выключено.

"Лаборатория Касперского" рекомендует участие в Kaspersky Security Network.

Также могут отображаться Положения KSN для управляемых приложений. Если вы принимаете условия использования Kaspersky Security Network, управляемое приложение отправляет данные в "Лабораторию Касперского". Если вы не принимаете условия использования Kaspersky Security Network, управляемое приложение не будет отправлять данные в "Лабораторию Касперского". Этот параметр можно изменить позже в свойствах политики приложения.

Нажмите на кнопку **Далее**, чтобы продолжить.

Шаг 6. Создание первоначальной конфигурации защиты

Вы можете проверить список созданных политик и задач.

Дождитесь завершения создания политик и задач и нажмите на кнопку **Далее**, чтобы продолжить. На последней странице мастера нажмите на кнопку **Готово** для выхода.

Опрос сегмента сети с помощью Kaspersky Security Center Cloud Console

Информацию о структуре сети и входящих в ее состав устройствах получает в ходе регулярных опросов облачных сегментов средствами AWS API, Azure API или Google API. На основании полученной информации Kaspersky Security Center Cloud Console обновляет состав и содержимое папок Нераспределенные устройства и Управляемые устройства. Если вы настроили автоматическое перемещение устройств в группы администрирования, обнаруженные в сети устройства включаются в состав групп администрирования.

Чтобы разрешить опрос облачных сегментов, необходимы соответствующие права, которые обеспечивает учетная запись IAM-пользователя (в AWS), идентификатор приложения и пароль (в Azure) или адрес электронной почты клиента Google, идентификатор проекта Google и закрытый ключ (в Google Cloud).

Вы можете добавлять и удалять соединения, а также настраивать для каждого облачного сегмента расписание опроса.

Добавление подключений для опроса облачных сегментов через Kaspersky Security Center Cloud Console

Чтобы добавить соединение для опроса облачных сегментов в список доступных:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Cloud**.

2. В появившемся окне нажмите **Свойства**.

3. В появившемся окне **Параметры** нажмите на кнопку **Добавить**.

   Откроется окно **Параметры облачного сегмента**.

4. Укажите имя облачного окружения для соединения, которое в дальнейшем будет использоваться для опроса облачного сегмента:

   - **Облачное окружение**

     Выберите облачное окружение, в котором вы разворачиваете Kaspersky Security Center Cloud Console: AWS, Azure или Google Cloud.

     Если вы планируете работать с несколькими облачными окружениями, выберите одно облачное окружение и потом запустите мастер еще раз.

   - **Название соединения**

     Введите имя для соединения. Название может содержать не более 256 символов. Допустимы только символы Юникод.

     Это имя будет также использоваться как имя группы администрирования для облачных устройств.

     Если вы планируете работать с несколькими облачными окружениями, возможно, вы захотите включить имя среды в название соединения, например, "Сегмент Azure", "Сегмент AWS" или "Сегмент Google".

5. Введите свои учетные данные, чтобы получить аутентификацию в облачном окружении, которое вы указали.

   - Если вы выбрали AWS, укажите следующее:

     - **ID ключа доступа**

       ID ключа доступа IAM – это последовательность из букв и цифр. Вы получили ID ключа при создании учетной записи IAM-пользователя.

       Поле доступно, если вы выбрали для авторизации ключ доступа AWS IAM.

     - **Секретный ключ**

       Секретный ключ, который вы получили с ID ключа доступа при создании учетной записи IAM-пользователя.

       Символы секретного ключа отображаются в виде звездочек. После того, как вы начали вводить секретный ключ, отображается кнопка **Показать**. Нажмите на эту кнопку и удерживайте ее необходимое вам время, чтобы просмотреть введенные символы.

       Поле доступно, если вы выбрали для авторизации ключ доступа AWS IAM.

Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

- Если вы выбрали Azure, укажите следующие параметры:

  - **Идентификатор приложения в Azure**

    Вы создали этот идентификатор приложения на портале Azure.

    Вы можете указать только один идентификатор приложения в Azure для опроса и других целей. Если необходимо опрашивать другой сегмент Azure, вам нужно сначала удалить первый сегмент в существующем соединении Azure.

  - **Идентификатор подписки Azure**

    Вы создали подписку на портале Azure.

  - **Пароль приложения Azure**

    Вы получили пароль к идентификатору приложения при создании ID приложения в Azure.

    Символы пароля отображаются в виде звездочек. После того, как вы начали вводить пароль, отображается кнопка **Показать**. Нажмите и удерживайте эту кнопку, чтобы просмотреть введенные символы.

    Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

  - **Имя учетной записи хранения Azure**

    Вы создали имя учетной записи хранения Azure для работы с Kaspersky Security Center Cloud Console.

  - **Ключ доступа хранилища Azure**

    Вы получили пароль (ключ) при создании учетной записи хранения Azure для работы с Kaspersky Security Center Cloud Console.

    Ключ доступен в разделе "Overview of the Azure storage account" в подразделе "Keys".

    Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

Если вы выбрали Google Cloud, укажите следующие параметры:

- **Электронная почта клиента**

  Электронная почта клиента – это адрес электронной почты, который вы использовали для регистрации вашего проекта в Google Cloud.

- **ID проекта**

  Идентификатор проекта – это идентификатор, полученный при регистрации проекта Google Cloud.

- **Закрытый ключ**

  Закрытый ключ – это последовательность символов, которые вы получили в качестве закрытого ключа при регистрации проекта в Google Cloud. Вы можете скопировать и вставить эту последовательность, чтобы избежать ошибок.

  Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

6. Нажмите на кнопку **Настроить расписание опроса**, чтобы изменить параметры по умолчанию.

Соединение сохранится в параметрах приложения.

После первого опроса нового облачного сегмента появится подгруппа в группе администрирования **Управляемые устройства\Cloud**, соответствующая этому сегменту.

Если вы указали неверные учетные данные, то инстансы не будут найдены во время опроса облачного сегмента, а новая подгруппа не будет отображаться в группе **Управляемые устройства\Cloud**.

Удаление соединения для опроса облачных сегментов

Если вам больше не нужно опрашивать какой-либо облачный сегмент, вы можете удалить соединение, соответствующее этому сегменту, из списка доступных. Вы также можете удалить соединение, если, например, права на опрос облачного сегмента перешли к другому пользователю с другими учетными данными.

Чтобы удалить соединение:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание → Обнаружение устройств → Cloud**.
2. В появившемся окне нажмите **Свойства**.
3. В открывшемся окне **Параметры** нажмите на имя сегмента, который вы хотите удалить.
4. Нажмите на кнопку **Удалить**.
5. В появившемся окне нажмите на кнопку **OK**, чтобы подтвердить свой выбор.

Соединение удалено. Устройства в облачном сегменте, соответствующие этому соединению, автоматически удаляются из групп администрирования.

Настройка расписания опроса с помощью Kaspersky Security Center Cloud Console

Опрос облачного сегмента происходит по расписанию. Вы можете задать периодичность, с которой происходит опрос.

На этапе работы мастера настройки для работы в облачном окружении автоматически задается периодичность опроса раз в пять минут. Вы можете изменить это значение в любое время и задать другое расписание. Не рекомендуется производить опрос чаще, чем раз в пять минут, так как это может привести к ошибкам в работе API.

Чтобы настроить расписание опроса облачного сегмента:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание → Обнаружение устройств → Cloud**.
2. В появившемся окне нажмите **Свойства**.

3. В открывшемся окне **Параметры** нажмите на имя сегмента, для которого вы хотите настроить расписание опроса.

   Откроется окно **Параметры облачного сегмента**.

4. В окне **Параметры облачного сегмента** нажмите на кнопку **Настроить расписание опроса**.

   Отобразится окно **Расписание**.

5. В окне **Расписание** укажите следующие параметры:

   - **Запуск по расписанию**

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

     - **По дням недели**

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

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

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

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

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

   - **Интервал запуска (сут)**

     Укажите значение N (для минут или дней).

   - **Начиная с момента**

     Укажите начало первого опроса.

   - **Запускать пропущенные задачи**

     Если ваша рабочая область выключена или недоступна в течение времени, на которое запланирован опрос, Kaspersky Security Center Cloud Console может либо начать опрос сразу после ее включения, либо дождаться следующего планового опроса.

     Если этот параметр включен, Kaspersky Security Center Cloud Console начинает опрос сразу после его того как рабочая область становится снова доступной.

     Если этот параметр выключен, Kaspersky Security Center Cloud Console ждет следующего планового опроса.

     По умолчанию параметр включен.

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

Расписание опроса для сегмента настроено и сохранено.

Просмотр результатов опроса облачного сегмента с помощью Kaspersky Security Center Cloud Console

Вы можете просмотреть результаты опроса облачного сегмента, то есть просмотреть список облачных устройств, управляемых Сервером администрирования.

Чтобы просмотреть результаты опроса облачного сегмента:

В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Cloud**.

Отображаются облачные сегменты, доступные для опроса.

Просмотр свойств облачных устройств с помощью Kaspersky Security Center Cloud Console

Вы можете просмотреть свойства каждого облачного устройства.

Чтобы просмотреть свойства облачного устройства:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Активы (Устройства)**.
2. Выберите устройство, свойства которого требуется просмотреть.

   В открывшемся окне свойств выберите раздел **Общие**.
3. Если вы хотите просмотреть свойства требуемых облачных устройств, в окне свойств выберите раздел **Система**.

   Свойства отображаются в зависимости от того, к какой облачной платформе принадлежит устройство.

   Для устройств в AWS отображаются следующие свойства:

   - **Устройство обнаружено с помощью API** (значение: **AWS**).
   - **Регион облачного окружения.**
   - **VPC.**
   - **Облачная зона доступности.**
   - **Облачная подсеть.**
   - **Облачная группа размещения** (это устройство отображается, если инстанс принадлежит группе размещения; в противном случае свойство не отображается).

Для устройств в Azure отображаются следующие свойства:

- **Устройство обнаружено с помощью API** (значение: **Microsoft Azure**).
- **Регион облачного окружения.**
- **Облачная подсеть.**

Для устройств в Google Cloud отображаются следующие свойства:

- **Устройство обнаружено с помощью API** (значение: **Google Cloud**).
- **Регион облачного окружения.**
- **VPC.**
- **Облачная зона доступности.**
- **Облачная подсеть.**

Синхронизация с облачным сегментом: настройка правила перемещения

Во время работы мастера настройки для работы в облачном окружении автоматически создается правило Синхронизация с облачным окружением. Правило позволяет автоматически перемещать устройства, найденные при каждом опросе, из группы Нераспределенные устройства в группу Управляемые устройства\Cloud, чтобы устройства были доступны для централизованного управления. По умолчанию правило включено после создания. Вы можете выключить, изменить или применить правило в любое время.

Чтобы изменить свойства правила Синхронизация с облачным окружением и/или применить правило:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Правила перемещения**.

   Откроется список правил перемещения.

2. В списке правил перемещения выберите **Синхронизация с облачным окружением**.

   Откроется окно свойств правила.

3. При необходимости укажите следующие параметры на вкладке **Условия правила** вкладки **Облачные сегменты**:

   - **Устройство находится в облачном сегменте**

     Если флажок установлен, то правило будет выполняться только для устройств, находящихся в выбранном сегменте.

     Если флажок снят, то правило будет выполняться для устройств, обнаруженных при опросе сети.

     По умолчанию флажок установлен.

   - **Включать дочерние объекты**

     Если флажок установлен, то правило будет выполняться для всех устройств в выбранном сегменте и во всех его вложенных облачных разделах.

Если флажок снят, то правило будет выполняться только для устройств, находящихся в корневом сегменте.

По умолчанию флажок установлен.

- **Перемещать устройства в соответствующие подгруппы**

  Если флажок установлен, то устройства из вложенных объектов перемещаются в подгруппы, соответствующие их структуре.

  Если флажок снят, то устройства из вложенных объектов перемещаются в корень подгруппы AWS без разбиения на подгруппы.

  По умолчанию флажок установлен.

- **Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств**

  Если флажок установлен, то если в структуре группы AWS нет подгруппы, соответствующей тому разделу, в котором находится устройство, программа создаст такую подгруппу.

  Если флажок снят, то программа не будет создавать новую подгруппу.

  По умолчанию флажок установлен.

- **Удалять подгруппы, для которых нет соответствия в облачных сегментах**

  Если флажок установлен, то программа удалит из группы AWS подгруппы, не соответствующие никаким облачным объектам.

  Если флажок снят, то подгруппы, не соответствующие облачным объектам, не будут удаляться.

  По умолчанию флажок установлен.

Если при работе с мастером настройки для работы в облачном окружении вы включили параметр **Синхронизировать группы администрирования с облачной структурой**, то правило **Синхронизация с облачным окружением** создается с включенными параметрами **Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств** и **Удалять подгруппы, для которых нет соответствия в облачных сегментах**.

Если вы не включили параметр **Синхронизировать группы администрирования с облачной структурой**, правило **Синхронизация с облачным окружением** создается с отключенными параметрами (флажки сняты). Если в процессе работы с Kaspersky Security Center Cloud Console вам потребуется, чтобы структура подгрупп группы **Управляемые устройства\Cloud** соответствовала структуре облачных сегментов, включите в свойствах правила параметры **Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств** и **Удалять подгруппы, для которых нет соответствия в облачных сегментах** и примените правило.

4. Выберите значение в раскрывающемся списке **Устройство обнаружено с помощью API**:

   - **Нет**. Устройство не обнаруживается с помощью AWS, Azure или Google API, то есть оно либо находится вне облачного окружения, либо находится в облачном окружении, но по каким-то причинам недоступно для поиска с помощью API.

   - **AWS**. Устройство обнаружено с использованием AWS API, то есть устройство находится в облачном окружении AWS.

   - **Azure**. Устройство обнаружено с использованием Azure API, то есть устройство находится в облачном окружении Azure.

- **Google Cloud**. Устройство обнаружено с использованием Google API, то есть устройство находится в облачном окружении Google Cloud.
- Не задано. Критерий не может быть применен.

5. При необходимости настройте другие свойства правила в других разделах.

Правило перемещения настроено.

Удаленная установка приложений на виртуальные машины Azure

У вас должна быть действующая лицензия для установки приложений на виртуальные машины Microsoft Azure.

Kaspersky Security Center Cloud Console поддерживает следующие сценарии:

- Клиентское устройство обнаружено с помощью Azure API; установка также выполняется средствами API. Использование Azure API означает, что вы можете установить только следующие приложения:
  - Kaspersky Endpoint Security для Linux
  - Kaspersky Endpoint Security для Windows
- Клиентское устройство обнаруживается с помощью Azure API; установка выполняется с помощью точки распространения или, если точки распространения нет, вручную с использованием автономных инсталляционных пакетов. Таким образом вы можете установить любое приложение, поддерживаемое Kaspersky Security Center Cloud Console.

Чтобы создать задачу удаленной установки приложения на виртуальные машины Azure:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. Следуйте далее указаниям мастера.
   a. Выберите тип задачи **Удаленная установка приложения**.
   b. На странице **Инсталляционные пакеты** выберите **Удаленная установка с помощью Microsoft Azure API**.
   c. При выборе учетной записи для доступа к устройствам используйте существующую учетную запись Azure или нажмите на кнопку **Добавить** и введите учетные данные своей учетной записи Azure:
      - **ИД приложения в Azure**

        Введите любое имя для учетных данных, которые вы указываете. Это имя отображается в списке учетных записей для запуска задачи.

- **Идентификатор приложения в Azure**

  Вы создали этот идентификатор приложения на портале Azure.

  Вы можете указать только один идентификатор приложения в Azure для опроса и других целей. Если необходимо опрашивать другой сегмент Azure, вам нужно сначала удалить первый сегмент в существующем соединении Azure.

- **Пароль приложения Azure**

  Вы получили пароль к идентификатору приложения при создании ID приложения в Azure.

  Символы пароля отображаются в виде звездочек. После того, как вы начали вводить пароль, отображается кнопка **Показать**. Нажмите и удерживайте эту кнопку, чтобы просмотреть введенные символы.

d. Выберите требуемые устройства из группы **Управляемые устройства\Cloud**.

После завершения работы мастера, задача удаленной установки приложения появится в списке задач.

Руководство по масштабированию

В этом руководстве представлена информация по масштабированию Kaspersky Security Center Cloud Console.

Об этом руководстве

Руководство по масштабированию Kaspersky Security Center (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;
- о расчетах для точек распространения:
  - об аппаратных требованиях к точкам распространения;
  - о расчетах количества и конфигурации.
- о настройке параметров сохранения событий в базе данных в зависимости от числа устройств в сети;
- общепринятые лучшие практики для оптимизации производительности;
- о настройке параметров некоторых задач для обеспечения оптимальной производительности Kaspersky Security Center;
- о потреблении трафика (нагрузке на сеть) между Сервером администрирования Kaspersky Security Center и каждым защищаемым устройством.

Рекомендуется обращаться к этому руководству в следующих ситуациях:

- при планировании ресурсов перед развертыванием решения Kaspersky Security Center;
- при планировании существенных изменений размеров сети, для управления защитой 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.

Лучшие практики для Сервера администрирования, управляющего большим количеством устройств

По умолчанию конфигурация рабочей области Kaspersky Security Center Cloud Console поддерживает защиту до 10 000 устройств. Если вам требуется защитить больше устройств, обратитесь в Службу технической поддержки, чтобы зарегистрировать рабочую область с увеличенным ограничением на количество устройств. В этом случае максимальное количество устройств в одной рабочей области увеличивается до 25 000.

Параметры политики и конфигурации по умолчанию предназначены для обеспечения стабильной и оптимальной работы Kaspersky Security Center Cloud Console. Изменение параметров рабочей области и управляемых приложений может снизить производительность решения. При планировании архитектуры учитывайте особенности сети, требования приложений и рекомендации.

Снижение производительности может привести к ошибкам подключения Агента администрирования на управляемых устройствах, замедлению работы Kaspersky Security Center Cloud Console, задержкам при загрузке страниц и навигации, медленному созданию и открытию объектов, а также замедлению сохранения изменений.

К признакам проблем с производительностью относятся следующие:

- Принудительные проверки с помощью утилиты klnagchk -sendhb и журнал событий Агента администрирования могут содержать ошибки, похожие на следующие:

  ```
  Попытка подключения к Серверу администрирования... При подключении к http://example.ksc.kaspersky.com:23456 произошла ошибка транспортного уровня: общая ошибка 0x4F4 (удаленный сервер занят).
  ```

- При проверке сетевого подключения к удаленному порту, используемому для приема подключений от Агента администрирования (например, с помощью telnet или Test-NetConnection), могут возникать ошибки.

Перед развертыванием и использованием Kaspersky Security Center Cloud Console рекомендуется ознакомиться с возможными проблемами в работе и приведенными ниже рекомендациями.

Лучшие практики для сокращения количества событий от управляемых устройств

В системе управления базами данных (СУБД) хранится до 400 000 событий. Каждые 10 минут Сервер администрирования проверяет, достигнуто ли ограничение на количество событий, и удаляет самые старые события, чтобы освободить место в базе данных. Если ведение журнала событий включено, записывается следующее событие: *Превышено ограничение числа событий, началось удаление событий из базы данных*.

Если управляемые устройства генерируют большое количество событий, автоматическое удаление может выполняться при каждой плановой проверке. Это может значительно снизить производительность Сервера администрирования. В этом случае для повышения производительности можно отключить хранение наиболее частых событий в базе данных.

Чтобы выключить хранение событий, генерируемых в большом количестве:

1. В главном окне приложения перейдите в раздел **Мониторинг → Панель мониторинга**.
2. Нажмите на кнопку **Добавить или восстановить виджет**.
3. В списке доступных виджетов нажмите на значок шеврона (>) рядом с категорией **Другое**, а затем выберите виджет **Десять наиболее частых событий базы данных**.
4. Нажмите на кнопку **Добавить**.
5. Используйте виджет **Десять наиболее частых событий базы данных** в панели мониторинга, чтобы узнать, какие события занимают больше всего места в базе данных.
6. Нажмите на событие в виджете, чтобы определить, какое приложение его сгенерировало.
7. Выключите хранение в базе данных этих событий во всех политиках и задачах соответствующего приложения.

Хранение часто генерируемых событий выключено.

Дополнительные рекомендации

- Настройте хранение в базе данных только важных событий. Для менее важных событий можно сократить срок хранения или полностью выключить хранение.
- Включайте события, которые обычно генерируются в большом количестве, только для ограниченного числа устройств. Для этого примените отдельную политику к устройствам, для которых требуются эти события.
- При разблокировке событий в разделе **Заблокированные частые события** отслеживайте и анализируйте количество новых полученных событий соответствующего типа.
- Используйте пересылку событий в SIEM-систему для долгосрочного хранения событий приложений "Лаборатории Касперского" на стороне SIEM-системы.
- При настройке параметров групповой задачи включите параметр **Сохранять только результат выполнения задачи**, чтобы сохранять только информацию о завершении задачи.
- Следуйте рекомендациям в разделе Хранение информации о событиях для задач и политик.

Лучшие практики для сокращения количества подключений от управляемых устройств

Недостаточное количество шлюзов соединения может привести к чрезмерной нагрузке на существующие шлюзы соединения и Сервер администрирования. При развертывании Kaspersky Security Center Cloud Console планируйте архитектуру с учетом топологии сети и ограничений пропускной способности.

Чтобы спланировать архитектуру или обновить существующую схему подключений, выполните следующие действия:

1. Ознакомьтесь с системными функциями Kaspersky Security Center Cloud Console по схеме в разделе Архитектура.
2. Рассчитайте минимально необходимое количество шлюзов соединения и точек распространения.
3. Настройте необходимое количество точек распространения в качестве шлюзов соединения для разных сегментов сети.
4. Настройте подключение управляемых устройств через шлюзы соединения.

Рекомендации по сокращению сетевого трафика, поступающего в корпоративную сеть и передаваемого между сегментами сети

- Используйте точки распространения, чтобы оптимизировать доставку обновлений антивирусных баз и инсталляционных пакетов приложений.
- Используйте прокси-сервер KSN на точках распространения, только если пропускная способность интернет-соединения ограничена. В остальных случаях рекомендуется прямое подключение к серверам KSN Cloud.
- Учитывайте ограничения пропускной способности между сегментами сети организации и обеспечьте постоянную доступность точек распространения на удаленных площадках.
- Настройте источники обновлений и расписания задач обновления антивирусных баз управляемых приложений.
- Последовательно устанавливайте новые версии приложений "Лаборатории Касперского" на группы устройств, чтобы распределить нагрузку на сеть во времени.
- Используйте уникальный IP-адрес многоадресной рассылки, чтобы оптимизировать доставку инсталляционных пакетов приложений на управляемые устройства в пределах области действия точки распространения.
- Оптимизируйте количество политик и профилей политик. Большое количество политик и профилей политик может замедлить распространение обновлений конфигурации приложений из-за увеличения объема передаваемых данных.

Другие лучшие практики

- При настройке **Параметры сетевого местоположения** в политиках Агента администрирования не указывайте порты Сервера администрирования для параметра **Условие для доступности адреса SSL-соединения**.
- Не выбирайте параметр **Применять правило постоянно** при создании или копировании правил перемещения устройств. Также избегайте использования правил, которые регулярно перемещают объекты устройств между группами администрирования.

- Выполняйте задачу **Инвентаризация** только на эталонных устройствах.
- Выключите получение информации о виртуальных машинах VDI.
- Ознакомьтесь с известными проблемами управляемых приложений, описанными в соответствующих разделах справки и описаниях компонентов приложений "Лаборатории Касперского".
- Учитывайте, что увеличение заданного по умолчанию значения в поле **Максимальное количество устройств, отображаемых в результатах распространения политики** может повлиять на производительность браузера.

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 Cloud Console, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Security Center Cloud Console.

Kaspersky предоставляет поддержку Kaspersky Security Center Cloud Console 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.

Информация, необходимая специалистам Службы технической поддержки "Лаборатории Касперского"

При обращении к специалистам Службы технической поддержки "Лаборатории Касперского" вас могут попросить предоставить следующую информацию:

- общую информацию о Kaspersky Security Center Cloud Console;
- идентификатор рабочей области;
- информацию о лицензии;
- количество установленных приложений;
- идентификатор и статус тенанта.

Вы можете найти эту информацию в Web Console, нажав на имя своей учетной записи, а затем в раскрывающемся списке, нажав на кнопку **Поддержка**. Вкладка **Общие** содержит информацию о вашей рабочей области, лицензировании и установленных приложениях. Скопируйте эту информацию и поделитесь ею со специалистами Службы технической поддержки "Лаборатории Касперского", чтобы получить помощь по вашему вопросу.

Источники информации о приложении

Страница Kaspersky Security Center Cloud Console на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Security Center Cloud Console вы можете получить общую информацию о приложении, его возможностях и особенностях работы.

Страница Kaspersky Security Center Cloud Console в Базе знаний

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

На странице Kaspersky Security Center Cloud Console 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 Cloud Console 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.

Известные проблемы и ограничения

Kaspersky Security Center Cloud Console имеет некоторые ограничения, которые не являются критичными для работы приложения:

- Переключение из режима Expert View в режим Pro View сейчас недоступно.
- На последнем этапе переключения из режима Pro View в режим Expert View страница в новом режиме может не загрузиться. Чтобы страница отображалась правильно, обновите ее.
- Центр уведомлений может не отображать уведомления о сбое шифрования диска на устройстве.
- При добавлении пользователя с главного Сервера администрирования на виртуальный Сервер администрирования ему автоматически назначается роль Главный администратор.

  Если вы хотите назначить пользователю специфические права (например, предоставить только право **Чтение**), перейдите в **Свойства Сервера администрирования**. На вкладке **Права доступа** выберите пользователей и виртуальный Сервер администрирования, а затем пропустите шаг назначения роли. Пользователи будут добавлены на виртуальный Сервер администрирования, но у них не будет прав на этом Сервере. Чтобы назначить пользователю специфические права, перейдите в свойства виртуального Сервера администрирования, выберите пользователей и назначьте им права.
- В разделе **Управление активами** → **Задачи** при выборе фильтра в столбце **Тип задачи** в раскрывающемся списке может отображаться одно неверное значение.
- Список политик отображается некорректно при изменении размера окна браузера.
- По умолчанию группировка по приложениям не включена в разделах **Политики** и **Задачи**.
- При многократном переключении из режима Pro View в Expert View политики для управляемых приложений создаются с повторяющимися именами.
- Информация о компонентах управляемых приложений недоступна, если Агент администрирования установлен на устройстве с операционной системой Windows XP.
- Вы не можете добавить инсталляционный пакет с одним и тем же языком локализации несколько раз. Например, если вы уже добавили инсталляционный пакет Kaspersky Endpoint Security для Windows (английский), вы можете добавить инсталляционные пакеты Kaspersky Endpoint Security для Windows на других языках, кроме английского.
- В окне **Детали алерта**, если вы переходите по любой ссылке, которая открывает другой раздел, а затем попытаетесь вернуться и нажать на кнопку **Назад** вашего браузера (или нажать **Alt**+**Влево**), окно **Детали алерта** не загружается.
- В локализации на упрощенном китайском информация в разделах **Мониторинг** → **MDR**, **Параметры** → **Интеграция** → **Kaspersky EDR Expert** и **Управление активами** → **Мобильные устройства** может отображаться некорректно.
- При импорте задачи *Загрузить обновления в хранилища точек распространения* или задачи *Проверка обновлений* параметр **Выбор устройств, которым будет назначена задача** включен. Эти задачи невозможно назначить выборкам устройств или заданным устройствам. Если вы назначите задачу *Загрузить обновления в хранилища точек распространения* или задачу *Проверка обновлений* на определенные устройства, задача будет импортирована некорректно.

- Если вы пытаетесь войти в Kaspersky Security Center Cloud Console с помощью служб Active Directory Federation Services (AD FS), но требуемые разрешения отсутствуют, Kaspersky Security Center Cloud Console по-прежнему возвращает ошибку "Недействительные учетные данные" вместо предупреждения о том, что у пользователя отсутствуют разрешения.

- Задача Управление устройствами не работает корректно для устройств с операционной системой macOS.

- В окне удаленной диагностики нажатие на кнопку **Скачать весь файл** может привести к неправильной загрузке.

- Игнорируемая уязвимость в приложениях сторонних производителей (кроме программного обеспечения Microsoft) не отображается на диаграмме **Статистика уязвимостей на устройствах**.

Глоссарий

AWS Application Program Interface (AWS API)

Программный интерфейс приложения платформы AWS, который используется приложением Kaspersky Security Center Cloud Console. Средствами AWS API проводится, в частности, опрос облачных сегментов и установка Агента администрирования на инстансы.

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*.

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.

IAM-пользователь

Пользователь сервисов AWS. IAM-пользователь может обладать правами на опрос облачного сегмента.

IAM-роль

Совокупность прав для выполнения запросов к сервисам AWS. IAM-роли не связаны ни с каким конкретным пользователем или группой и обеспечивают права доступа без использования ключей доступа IAM AWS. IAM-роль можно присвоить пользователям IAM, инстансам EC2, приложениям или сервисам AWS.

Identity and Access Management (IAM)

Сервис AWS, который позволяет управлять доступом пользователей к другим сервисам и ресурсам AWS.

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 Cloud Console

Приложение для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Kaspersky Security Center Cloud Console размещается и поддерживается в инфраструктуре "Лаборатории Касперского". Приложение входит в состав облачного решения Kaspersky. В рамках этого решения также можно использовать Kaspersky Next Pro View.

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к постоянно обновляемой 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.

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.

Push-сервер

Функция точки распространения, позволяющая поддерживать постоянное соединение между управляемыми устройствами и Сервером администрирования. Это необходимо для получения информации от устройств и для немедленного выполнения команд управления.

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 Cloud Console, 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.

Администратор Kaspersky Security Center Cloud Console

Лицо, управляющее работой приложения через систему удаленного централизованного администрирования Kaspersky Security Center Cloud Console.

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-плагин управления

Специальный компонент, используемый для удаленного управления приложениями "Лаборатории Касперского" с помощью Kaspersky Security Center Cloud Console. Плагин управления представляет собой интерфейс между Kaspersky Security Center Cloud Console и определенным приложением "Лаборатории Касперского". С помощью плагина управления можно настраивать задачи и политики для приложения.

Виртуальный Сервер администрирования

Компонент приложения Kaspersky Security Center Cloud Console, 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:

- Виртуальные Сервера администрирования могут функционировать только в составе подчиненных Серверов 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.

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.

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 Cloud Console. 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.

Инстанс Amazon EC2

Виртуальная машина, созданная на основе образа AMI с использованием Amazon Web Services.

Карантин

Папка, в которую приложение "Лаборатории Касперского" перемещает обнаруженные возможно зараженные объекты. Объекты на карантине хранятся в зашифрованном виде во избежание их воздействия на компьютер.

Ключ доступа IAM AWS

Комбинация, состоящая из ID ключа (вида "AKIAIOSFODNN7EXAMPLE") и секретного ключа (вида "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"). Пара принадлежит IAM-пользователю и используется для получения доступа к сервисам AWS.

Консоль AWS

Веб-интерфейс для управления инстансами Amazon EC2. Консоль AWS доступна в интернете на странице https://aws.amazon.com/console/.

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.

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 Cloud Console.

Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений "Лаборатории Касперского".

Образ AMI

Шаблон с необходимой для запуска виртуальной машины конфигурацией программного обеспечения. На основе одного образа AMI можно создать несколько инстансов.

Оператор Kaspersky Security Center Cloud Console

Пользователь, который ведет наблюдение за состоянием и работой системы защиты, управляемой при помощи Kaspersky Security Center Cloud Console.

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.

Порог вирусной активности

Максимально допустимое количество событий заданного типа в течение ограниченного времени, превышение которого будет считаться повышением вирусной активности и возникновением угрозы вирусной атаки. Данная характеристика имеет большое значение в периоды вирусных эпидемий и позволяет администратору своевременно реагировать на возникающие угрозы вирусных атак.

Профиль политики

Именованное подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – условия активации профиля.

Рабочая область

Виртуальный сервер администрирования "Лаборатории Касперского" для управления приложениями безопасности на устройствах, подключенных к Kaspersky Security Center Cloud Console, а также для хранения индивидуальных параметров Kaspersky Security Center Cloud Console и регистрационных данных компании, использующей это программное решение.

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.

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.

Тег приложения

Метка приложения, которую можно использовать для группировки и поиска приложений. Назначенный приложению тег можно использовать в условиях для выборок устройств.

Тег устройства

Метка устройства, которую можно использовать для группировки, описания, поиска устройств.

Удаленная установка

Установка приложений "Лаборатории Касперского" при помощи инструментов, предоставляемых приложением Kaspersky Security Center Cloud Console.

Управляемое устройство

Устройство с установленным приложением безопасности, подключенное к Kaspersky Security Center Cloud Console.

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.

Устройство с защитой на уровне UEFI

Устройство со встроенным на уровне BIOS программным обеспечением Антивирус Касперского для UEFI. Встроенная защита обеспечивает безопасность устройства еще с начала запуска системы, в то время как защита устройств, не имеющих встроенного ПО, начинает действовать только после запуска приложения защиты.

Учетная запись Kaspersky Security Center Cloud Console

Учетная запись, необходимая для настройки Kaspersky Security Center Cloud Console путем добавления и удаления учетных записей пользователей и настройки профилей безопасности (политик безопасности). Эта учетная запись позволяет использовать службу My Kaspersky. Эта учетная запись создается, когда вы начинаете пользоваться Kaspersky Security Center Cloud Console.

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.

Форсированная установка

Метод удаленной установки приложения "Лаборатории Касперского", который позволяет провести удаленную установку программного обеспечения на конкретные клиентские устройства. Для успешного выполнения задачи методом форсированной установки учетная запись для запуска задачи должна обладать правами на удаленный запуск приложений на клиентских устройствах. Данный метод рекомендуется для установки приложений на устройства, работающие под управлением операционных систем Microsoft Windows NT / 2000 / 2003 / XP, в которых поддерживается такая возможность.

Хранилище событий

Часть базы данных Сервера администрирования, предназначенная для хранения информации о событиях, которые возникают в Kaspersky Security Center Cloud Console.

Централизованное управление приложением

Удаленное управление приложением при помощи сервисов администрирования, предоставляемых Kaspersky Security Center Cloud Console.

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.

Файл legal_notices.txt также находится в папке установки управляемых приложений.

Trademark notices

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe, Acrobat, Flash, PostScript, Reader, Shockwave являются либо зарегистрированными товарными знаками, либо товарными знаками компании Adobe в США и/или других странах.

AMD64 – товарный знак или зарегистрированный товарный знак Advanced Micro Devices, Inc.

Amazon, Amazon EC2, Amazon Web Services, AWS and 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, App Store, AppleScript, FileVault, iPadOS, iPhone, iTunes, Mac, Mac OS, macOS, OS X, Safari, and QuickTime – 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, IOS, Cisco Jabber 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.

Cloudflare, логотип Cloudflare и Cloudflare Workers являются товарными знаками и/или зарегистрированными товарными знаками компании Cloudflare, Inc. в США и других юрисдикциях.

Corel, and CorelDRAW – товарные знаки или зарегистрированные в Канаде, США и/или других странах товарные знаки Corel Corporation и/или ее дочерних компаний.

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, Dalvik, Firebase, Google Chrome, Google Earth, Google Maps, Google Play, Google Public DNS – товарные знаки Google LLC.

HUAWEI, EulerOS, HUAWEI CLOUD являются товарными знаками Huawei Technologies Co., Ltd.

Intel and Core 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, ActiveX, BitLocker, Excel, Hyper-V, InfoPath, Internet Explorer, Microsoft 365, Microsoft Edge, MS-DOS, MultiPoint, Office 365, OneNote, Outlook, PowerPoint, PowerShell, Segoe, Skype, SQL Server, Tahoma, Visio, Win32, Windows, Windows Azure, Windows Media, Windows Mobile, Windows Phone, Windows Server, and Windows Vista являются товарными знаками группы компаний Microsoft.

CVE – зарегистрированный товарный знак MITRE Corporation.

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.

NetWare – товарный знак Novell Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

OpenVPN – зарегистрированный товарный знак OpenVPN, Inc.

Oracle, Java, JavaScript – зарегистрированные товарные знаки компании Oracle и/или аффилированных компаний.

Parallels, логотип Parallels и Coherence являются товарными знаками или зарегистрированными товарными знаками Parallels International GmbH.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

Red Hat, Red Hat Enterprise Linux, CentOS, Fedora – товарные знаки или зарегистрированные в США и других странах товарные знаки 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.

SAMSUNG – товарный знак компании SAMSUNG в США или других странах.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

Splunk – товарный знак и зарегистрированный в США и других странах товарный знак 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.

Rocky Linux является товарным знаком The Rocky Enterprise Software Foundation.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.