kaspersky

Kaspersky Security Center 15.1 Windows

© 2026 АО "Лаборатория Касперского"

Содержание

Справка Kaspersky Security Center 15.1

Что нового

Исправленные ошибки

О Kaspersky Security Center

- Архитектура
- Аппаратные и программные требования
  - Требования Сервера администрирования
  - Требования Web Console
  - Требования серверов мобильных устройств
  - Требования Консоли администрирования
  - Требования Агента администрирования
- Совместимые приложения и решения "Лаборатории Касперского"
- Лицензии и возможности Kaspersky Security Center 15.1
- О совместимости компонентов Kaspersky Security Center
- Сравнение версий Kaspersky Security Center: на базе Windows и на базе Linux
- О Kaspersky Security Center Cloud Console

Kaspersky Security Center 15.1

- Основные понятия
  - Сервер администрирования
  - Иерархия Серверов администрирования
  - Виртуальный Сервер администрирования
  - Сервер мобильных устройств
  - Веб-сервер
  - Агент администрирования
  - Группы администрирования
  - Управляемое устройство
  - Нераспределенное устройство
  - Рабочее место администратора
  - Плагин управления
  - Веб-плагин управления
  - Политики
  - Профили политик
  - Tasks
  - Область действия задачи
  - Взаимосвязь политики и локальных параметров приложения
  - Точка распространения
  - Шлюз соединения
- Основной сценарий установки
- Порты, используемые Kaspersky Security Center
- Сертификаты для работы с Kaspersky Security Center
  - О сертификатах Kaspersky Security Center
  - О сертификате Сервера администрирования
  - Требования к пользовательским сертификатам, используемым в Kaspersky Security Center

Сценарий: задание пользовательского сертификата Сервера администрирования
Замена сертификата Сервера администрирования с помощью утилиты klsetsrvcert
Подключение Агентов администрирования к Серверу администрирования с помощью утилиты klmover
Перевыпуск сертификата Веб-сервера
Схемы трафика данных и использования портов
Сервер администрирования и управляемые устройства в локальной сети (LAN)
Главный Сервер администрирования в локальной сети (LAN) и два подчиненных Сервера администрирования
Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете: использование обратного прокси-сервера
Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете: использование шлюза соединения
Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения
Условные обозначения в схемах взаимодействия
Сервер администрирования и СУБД
Сервер администрирования и Консоль администрирования
Сервер администрирования и клиентское устройство: Управление приложением безопасности
Обновление программного обеспечения на клиентском устройстве с помощью точки распространения
Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования
Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне
Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство
Сервер администрирования и два устройства в демилитаризованной зоне: шлюз соединений и клиентское устройство
Сервер администрирования и Kaspersky Security Center Web Console
Активация и управление приложением безопасности на мобильном устройстве
Лучшие практики развертывания
Руководство по усилению защиты
Развертывание Сервера администрирования
Безопасность соединения
Учетные записи и авторизация
Управление защитой Сервера администрирования
Управление защитой Агента администрирования
Управление защитой клиентских устройств
Настройка защиты управляемых приложений
Обслуживание Сервера администрирования
Передача событий в сторонние системы
Рекомендации по безопасности сторонних информационных систем
Рекомендации по использованию приложений безопасности "Лаборатории Касперского"
Подготовка к развертыванию
Планирование развертывания Kaspersky Security Center
Типовые способы развертывания системы защиты
О планировании развертывания Kaspersky Security Center в сети организации
Выбор структуры защиты организации
Типовые конфигурации Kaspersky Security Center
Типовая конфигурация: один офис
Типовая конфигурация: несколько крупных офисов с собственными администраторами
Типовая конфигурация: множество небольших удаленных офисов

Выбор СУБД для Сервера администрирования
Применение накопительного исправления CU12 при использовании SQL Server 2019 в качестве СУБД
Настройка сервера MariaDB x64 для работы с Kaspersky Security Center 15.1
Настройка сервера MySQL x64 для работы с Kaspersky Security Center 15.1
Настройка сервера PostgreSQL или Postgres Pro для работы с Kaspersky Security Center 15.1
Управление мобильными устройствами с установленным Kaspersky Endpoint Security для Android
Предоставление доступа к Серверу администрирования из интернета
Доступ из интернета: Сервер администрирования в локальной сети
Доступ из интернета: Сервер администрирования в демилитаризованной зоне
Доступ из интернета: Агент администрирования в качестве шлюза соединения в демилитаризованной зоне
О точках распространения
Увеличение ограничения дескрипторов файлов для службы klnagent
Расчет количества и конфигурации точек распространения
Иерархия Серверов администрирования
Виртуальные Серверы администрирования
Информация об ограничениях Kaspersky Security Center
Нагрузка на сеть
Первоначальное развертывание антивирусной защиты
Первоначальное обновление антивирусных баз
Синхронизация клиента с Сервером администрирования
Дополнительное обновление антивирусных баз
Обработка событий клиентов Сервером администрирования
Расход трафика за сутки
Подготовка к управлению мобильными устройствами
Сервер iOS MDM
Типовая конфигурация: Kaspersky Device Management для iOS в демилитаризованной зоне
Типовая конфигурация: Сервер iOS MDM в локальной сети организации
Управление мобильными устройствами с установленным Kaspersky Endpoint Security для Android
Сведения о производительности Сервера администрирования
Ограничения подключений к Серверу администрирования
Результаты тестов производительности Сервера администрирования
Результаты тестирования производительности прокси-сервера KSN
Сетевые параметры для взаимодействия с внешними сервисами
Развертывание Агента администрирования и приложения безопасности
Первоначальное развертывание
Настройка параметров инсталляторов
Инсталляционные пакеты
Свойства MSI и файлы трансформации
Развертывание при помощи сторонних средств удаленной установки приложений
О задачах удаленной установки приложений Kaspersky Security Center
Развертывание захватом и копированием образа устройства
Неверно выполнено копирование образа жесткого диска
Развертывание с помощью механизма групповых политик Microsoft Windows
Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center
Запуск автономных пакетов, сформированных Kaspersky Security Center
Возможности ручной установки приложений
Создание MST-файла

Удаленная установка приложений на устройства с установленным Агентом администрирования
Управление перезагрузкой устройств в задаче удаленной установки
Целесообразность обновления баз в инсталляционном пакете приложения безопасности
Использование средств удаленной установки приложений Kaspersky Security Center для запуска на управляемых устройствах произвольных исполняемых файлов
Мониторинг развертывания
Настройка параметров инсталляторов
Общая информация
Установка в тихом режиме (с файлом ответов)
Установка Агента администрирования в тихом режиме (без файла ответов)
Частичная настройка параметров установки через setup.exe
Параметры установки Сервера администрирования
Параметры установки Агента администрирования
Виртуальная инфраструктура
Рекомендации по снижению нагрузки на виртуальные машины
Поддержка динамических виртуальных машин
Поддержка копирования виртуальных машин
Поддержка отката файловой системы для устройств с Агентом администрирования
Локальная установка приложений
Локальная установка Агента администрирования
Установка Агента администрирования в тихом режиме
Установка Агента администрирования для Linux в тихом режиме (с файлом ответов)
Подготовка устройства под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования
Установка Агента администрирования для Linux в интерактивном режиме
Локальная установка плагина управления приложением
Установка приложений в тихом режиме
Установка приложений с помощью автономных пакетов
Параметры инсталляционного пакета Агента администрирования
Просмотр Политики конфиденциальности
Развертывание систем управления мобильными устройствами
Развертывание системы управления по протоколу iOS MDM
Установка Сервера iOS MDM
Установка Сервера iOS MDM в тихом режиме
Схемы развертывания Сервера iOS MDM
Упрощенная схема развертывания
Схема развертывания с использованием принудительного делегирования Kerberos Constrained Delegation (KCD)
Получение APNs-сертификата
Обновление APNs-сертификата
Настройка резервного сертификата Сервера iOS MDM
Установка APNs-сертификата на Сервер iOS MDM
Настройка доступа к сервису Apple Push Notification
Выписка и установка общего сертификата на мобильное устройство
Добавление KES-устройства в список управляемых устройств

Подключение KES-устройств к Серверу администрирования
Прямое подключение устройств к Серверу администрирования
Схема подключения KES-устройств к Серверу с использованием принудительного делегирования Kerberos (KCD)
Использование Firebase Cloud Messaging
Интеграция с инфраструктурой открытых ключей
Веб-сервер Kaspersky Security Center
Установка Kaspersky Security Center
Подготовка к установке
Учетные записи для работы с СУБД
Настройка учетных записей для работы с SQL Server (аутентификация Windows)
Настройка учетных записей для работы с SQL Server (аутентификация SQL Server)
Настройка учетных записей для работы с MySQL и MariaDB
Перенос данных из общего табличного пространства в табличное пространство file-per-table в СУБД MySQL или MariaDB
Настройка учетных записей для работы с PostgreSQL и Postgres Pro
Сценарий: аутентификация Microsoft SQL Server
Сценарий: аутентификация MySQL Server
Сценарий: аутентификация PostgreSQL Server
Рекомендации по установке Сервера администрирования
Создание учетных записей для служб Сервера администрирования на отказоустойчивом кластере
Задание папки общего доступа
Удаленная установка средствами Сервера администрирования с помощью групповых политик Active Directory
Удаленная установка рассылкой UNC-пути на автономный пакет
Обновление из общей папки Сервера администрирования
Установка образов операционных систем
Указание адреса Сервера администрирования
Стандартная установка
Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности
Шаг 2. Выбор типа установки
Шаг 3. Установка Kaspersky Security Center Web Console
Шаг 4. Выбор размера сети
Шаг 5. Выбор базы данных
Шаг 6. Настройка параметров SQL-сервера
Шаг 7. Выбор режима аутентификации
Шаг 8. Распаковка и установка файлов на жесткий диск
Выборочная установка
Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности
Шаг 2. Выбор типа установки
Шаг 3. Выбор компонентов для установки
Шаг 4. Установка Kaspersky Security Center Web Console
Шаг 5. Выбор размера сети
Шаг 6. Выбор базы данных
Шаг 7. Настройка параметров SQL-сервера
Шаг 8. Выбор режима аутентификации
Шаг 9. Выбор учетной записи для запуска Сервера администрирования
Шаг 10. Выбор учетной записи для запуска служб Kaspersky Security Center

Шаг 11. Определение папки общего доступа
Шаг 12. Настройка параметров подключения к Серверу администрирования
Шаг 13. Задание адреса Сервера администрирования
Шаг 14. Адрес Сервера для подключения мобильных устройств
Шаг 15. Выбор плагинов управления приложениями
Шаг 16. Распаковка и установка файлов на жесткий диск
Развертывание отказоустойчивого кластера Kaspersky Security Center
Сценарий: развертывание отказоустойчивого кластера Kaspersky Security Center
Об отказоустойчивом кластере Kaspersky Security Center
Подготовка файлового сервера для отказоустойчивого кластера Kaspersky Security Center
Подготовка узлов для отказоустойчивого кластера Kaspersky Security Center
Установка Kaspersky Security Center на узлы отказоустойчивого кластера Kaspersky Security Center
Запуск и остановка узлов кластера вручную
Установка Сервера администрирования на отказоустойчивом кластере Windows Server
Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности
Шаг 2. Выбор типа установки на кластер
Шаг 3. Указание имени виртуального Сервера администрирования
Шаг 4. Указание параметров сети виртуального Сервера администрирования
Шаг 5. Указание группы кластеров
Шаг 6. Выбор кластерного хранилища данных
Шаг 7. Указание учетной записи для удаленной установки
Шаг 8. Выбор компонентов для установки
Шаг 9. Выбор размера сети
Шаг 10. Выбор базы данных
Шаг 11. Настройка параметров SQL-сервера
Шаг 12. Выбор режима аутентификации
Шаг 13. Выбор учетной записи для запуска Сервера администрирования
Шаг 14. Выбор учетной записи для запуска служб Kaspersky Security Center
Шаг 15. Определение папки общего доступа
Шаг 16. Настройка параметров подключения к Серверу администрирования
Шаг 17. Задание адреса Сервера администрирования
Шаг 18. Адрес Сервера для подключения мобильных устройств
Шаг 19. Распаковка и установка файлов на жесткий диск
Установка Сервера администрирования в тихом режиме
Установка Консоли администрирования на рабочее место администратора
Изменения в системе после установки Kaspersky Security Center
Удаление приложения
Об обновлении предыдущей версии Kaspersky Security Center
Обновление предыдущей версии Kaspersky Security Center
Обновление Kaspersky Security Center на узле отказоустойчивого кластера Kaspersky Security Center
Обновление Kaspersky Security Center на узлах отказоустойчивого кластера Microsoft
Первоначальная настройка Kaspersky Security Center
Руководство по усилению защиты
Мастер первоначальной настройки Сервера администрирования
О мастере первоначальной настройки
Запуск мастера первоначальной настройки Сервера администрирования
Шаг 1. Настройка параметров прокси-сервера

Шаг 2. Выбор способа активации приложения
Шаг 3. Выбор областей защиты и операционных систем
Шаг 4. Выбор плагинов для управляемых приложений
Шаг 5. Загрузка дистрибутивов и создание инсталляционных пакетов
Шаг 6. Настройка использования Kaspersky Security Network
Шаг 7. Настройка параметров отправки уведомлений по электронной почте
Шаг 8. Настройка параметров управления обновлениями
Шаг 9. Создание первоначальной конфигурации защиты
Шаг 10. Подключение мобильных устройств
Шаг 11. Загрузка обновлений
Шаг 12. Обнаружение устройств
Шаг 13. Завершение работы мастера первоначальной настройки
Настройка подключения Консоли администрирования к Серверу администрирования
Настройка параметров доступа Сервера администрирования к интернету
Подключение автономных устройств
Сценарий: подключение автономных устройств через шлюз соединения
Сценарий: подключение автономных устройств через подчиненный Сервер администрирования в демилитаризованной зоне
О подключении автономных устройств
Подключение внешних настольных устройств к Серверу администрирования
О профилях соединения для автономных пользователей
Создание профиля соединения для автономных пользователей
О переключении Агента администрирования на другой Сервер администрирования
Создание правила переключения Агента администрирования по сетевому местоположению
Уведомления о событиях
Настройка параметров уведомлений о событиях
Проверка распространения уведомлений
Уведомление о событиях с помощью исполняемого файла
Шифрование подключения TLS
Настройка интерфейса
Обнаружение устройств в сети
Сценарий: обнаружение сетевых устройств
Нераспределенные устройства
Обнаружение устройств
Опрос сети Windows
Опрос Active Directory
Опрос IP-диапазонов
Опрос Zeroconf
Работа с Windows-доменами Просмотр и изменение параметров домена
Настройка правил хранения для нераспределенных устройств
Работа с IP-диапазонами
Создание IP-диапазона
Просмотр и изменение параметров IP-диапазона
Работа с группами Active Directory. Просмотр и изменение параметров группы
Создание правил автоматического перемещения устройств в группы администрирования

Использование динамического режима VDI на клиентских устройствах
Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования
Поиск устройств, являющихся частью VDI
Перемещение в группу администрирования устройств, являющихся частью VDI
Инвентаризация оборудования
Добавление информации о новых устройствах
Настройка критериев определения корпоративных устройств
Настройка пользовательских полей
Лицензирование
События превышения лицензионного ограничения
О лицензировании
О лицензии
О Лицензионном соглашении
О Лицензионном сертификате
О лицензионном ключе
О файле ключа
О подписке
О коде активации
Отзыв согласия с Лицензионным соглашением
О предоставлении данных
Варианты лицензирования Kaspersky Security Center
Особенности лицензирования Kaspersky Security Center и управляемых приложений
Приложения "Лаборатории Касперского". Централизованное развертывание
Замещение приложений безопасности сторонних производителей
Установка приложений с помощью задачи удаленной установки
Установка приложения на выбранные устройства
Установка приложения на клиентские устройства группы администрирования
Установка приложения с помощью групповых политик Active Directory
Удаленная установка приложений на устройства с операционной системой macOS
Установка приложений на подчиненные Серверы администрирования
Установка приложений с помощью мастера удаленной установки
Работа с плагинами управления
Просмотр отчета о развертывании защиты
Удаленная деинсталляция приложений
Удаленная деинсталляция приложения с клиентских устройств группы администрирования
Удаленная деинсталляция приложения с выбранных устройств
Работа с инсталляционными пакетами
Создание инсталляционного пакета.
Создание автономного инсталляционного пакета
Создание пользовательского инсталляционного пакета
Просмотр и изменение свойств пользовательских инсталляционных пакетов
Получение инсталляционного пакета Агента администрирования из комплекта поставки Kaspersky Security Center
Распространение инсталляционных пакетов на подчиненные Серверы администрирования
Распространение инсталляционных пакетов с помощью точек распространения
Передача в Kaspersky Security Center информации о результатах установки приложения
Определение адреса прокси-сервера KSN для инсталляционных пакетов
Получение актуальных версий приложений

Подготовка устройства под управлением Windows к удаленной установке
Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux
Подготовка устройства под управлением SUSE Linux Enterprise Server 15 к установке Агента администрирования
Подготовка устройства с операционной системой macOS к удаленной установке Агента администрирования
Приложения "Лаборатории Касперского": лицензирование и активация
Лицензирование управляемых приложений
Просмотр информации об используемых лицензионных ключах
Добавление лицензионного ключа в хранилище Сервера администрирования
Удаление лицензионного ключа Сервера администрирования
Распространение лицензионного ключа на клиентские устройства
Автоматическое распространение лицензионного ключа
Создание и просмотр отчета об использовании лицензионных ключей
Просмотр информации о лицензионных ключах приложения
Экспорт файла ключа
Настройка защиты сети
Сценарий: настройка защиты сети
Настройка и распространение политик: подход, ориентированный на устройства
Подходы к управлению безопасностью, ориентированные на устройства и на пользователей
Ручная настройка политики Kaspersky Endpoint Security
Настройка политики в разделе Продвинутая защита
Настройка политики в разделе Базовая защита
Настройка политики в разделе Дополнительные параметры
Настройка политики в разделе Настройка событий
Ручная настройка групповой задачи обновления Kaspersky Endpoint Security
Ручная настройка групповой задачи проверки устройства Kaspersky Endpoint Security
Настройка расписания задачи Поиск уязвимостей и требуемых обновлений.
Ручная настройка групповой задачи установки обновлений и закрытия уязвимостей
Настройка количества событий в хранилище событий
Установка максимального срока хранения информации о закрытых уязвимостях
Управление задачами
Создание задачи
Создание задачи Сервера администрирования
Создание задачи для набора устройств
Создание локальной задачи
Отображение унаследованной групповой задачи в рабочей области вложенной группы
Автоматическое включение устройств перед запуском задачи
Автоматическое выключение устройства после выполнения задачи
Ограничение времени выполнения задачи
Экспорт задачи
Импорт задачи
Конвертация задач
Запуск и остановка задачи вручную
Приостановка и возобновление задачи вручную
Наблюдение за ходом выполнения задачи
Просмотр результатов выполнения задач, хранящихся на Сервере администрирования
Настройка фильтра информации о результатах выполнения задачи

Изменение задачи. Откат изменений
Сравнение задач
Учетные записи для запуска задач
Экспорт результатов выполнения задачи
Мастер изменения паролей задач
Шаг 1. Выбор учетных данных
Шаг 2. Выбор выполняемого действия
Шаг 3. Просмотр результатов
Создание иерархии групп администрирования, подчиненных виртуальному Серверу администрирования
Политики и профили политик
Иерархия политик, использование профилей политик
Иерархия политик
Профили политик
Наследование параметров политики
Управление политиками
Создание политики
Отображение унаследованной политики во вложенной группе
Активация политики
Автоматическая активация политики по событию "Вирусная атака"
Применение политики для автономных пользователей
Изменение политики. Откат изменений
Сравнение политик
Просмотр диаграммы состояния применения политики
Удаление политики
Копирование политики
Экспорт политики
Импорт политики
Конвертация политик
Управление профилями политик
Создание профиля политики
Изменение профиля политики
Удаление профиля политики
Создание правила активации профиля политики
Правила перемещения устройств
Копирование правил перемещения устройств
Категоризация программного обеспечения
Необходимые условия для установки приложений на устройства организации-клиента
Просмотр и изменение локальных параметров приложения
Обновление Kaspersky Security Center и управляемых приложений
Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"
Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"
Об использовании файлов различий для обновления баз и модулей приложений "Лаборатории Касперского"
Включение функции загрузки файлов различий
Создание задачи для загрузки обновлений в хранилище Сервера администрирования
Создание задачи загрузки обновлений в хранилища точек распространения
Настройка параметров задачи загрузки обновлений в хранилище Сервера администрирования
Проверка полученных обновлений

Настройка проверочных политик и вспомогательных задач
Просмотр полученных обновлений
Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства
Офлайн-модель получения обновлений
Включение и выключение офлайн-модели получения обновлений
Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center
Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center
Автоматическое распространение обновлений
Автоматическое распространение обновлений на клиентские устройства
Автоматическое распространение обновлений на подчиненные Серверы администрирования
Автоматическое назначение точек распространения
Назначение устройства точкой распространения вручную
Удаление устройства из списка точек распространения
Загрузка обновлений точками распространения
Удаление обновлений программного обеспечения из хранилища
Установка патча для приложения "Лаборатории Касперского" в кластерной модели
Управление приложениями сторонних производителей на клиентских устройствах
О приложениях сторонних производителей
Установка обновлений приложений сторонних производителей
Сценарий: обновление приложений сторонних производителей
Просмотр информации о доступных обновлениях для приложений сторонних производителей
Одобрение и отклонение обновлений программного обеспечения
Синхронизация обновлений Windows Update с Сервером администрирования
Шаг 1. Определение необходимости уменьшения трафика
Шаг 2. Приложения
Шаг 3. Категории обновлений
Шаг 4. Языки локализации обновлений
Шаг 5. Выбор учетной записи для запуска задачи
Шаг 6. Настройка расписания запуска задачи
Шаг 7. Определение названия задачи
Шаг 8. Завершение создания задачи
Установка обновлений на устройства вручную
Настройка обновлений Windows в политике Агента администрирования
Закрытие уязвимостей в приложениях сторонних производителей
Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей
Об обнаружении и закрытии уязвимостей в приложениях
Просмотр информации об уязвимостях в приложениях
Просмотр статистики уязвимостей на управляемых устройствах.
Поиск уязвимостей в приложениях
Закрытие уязвимостей в приложениях
Закрытие уязвимостей в изолированной сети
Сценарий: закрытие уязвимостей в приложениях сторонних производителей в изолированной сети
О закрытии уязвимостей в приложениях сторонних производителей в изолированной сети
Настройка Сервера администрирования с доступом в интернет для закрытия уязвимостей в изолированной сети
Настройка изолированных Серверов администрирования для закрытия уязвимостей в изолированной сети

Передача исправлений и установка обновлений в изолированной сети
Выключение возможности передачи исправлений и установки обновлений в изолированной сети
Игнорирование уязвимостей в приложениях
Пользовательские исправления для уязвимостей в приложениях сторонних производителей
Правила установки обновлений
Группы приложений
Использование компонента Контроль приложений для управления исполняемыми файлами
Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах
Создание категорий приложений для политики Kaspersky Endpoint Security для Windows
Создание пополняемой вручную категории приложений
Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств
Создание категории приложений, в которую входят исполняемые файлы из указанных папок
Добавление исполняемых файлов, связанных с событием, в категорию приложения
Настройка управления запуском приложений на клиентских устройствах
Просмотр результатов статического анализа правил запуска исполняемых файлов
Просмотр реестра приложений
Изменение времени начала инвентаризации программного обеспечения
Создание групп лицензионных приложений
Управление лицензионными ключами для групп лицензионных приложений
Инвентаризация исполняемых файлов
Просмотр информации об исполняемых файлах
Мониторинг и отчеты
Сценарий: мониторинг и отчеты
Мониторинг цветовых индикаторов и зарегистрированных событий в Консоли администрирования
Работа с отчетами, статистикой и уведомлениями
Работа с отчетами
Создание шаблона отчета
Просмотр и изменение свойств шаблона отчета
Расширенный формат фильтра в шаблонах отчета
Конвертация фильтра в расширенный формат
Настройка расширенного фильтра
Создание и просмотр отчета
Сохранение отчета
Создание задачи рассылки отчета
Шаг 1. Выбор типа задачи
Шаг 2. Выбор типа отчета
Шаг 3. Действия над отчетом
Шаг 4. Выбор учетной записи для запуска задачи
Шаг 5. Настройка расписания задачи
Шаг 6. Определение названия задачи
Шаг 7. Завершение создания задачи
Работа со статистической информацией
Настройка параметров уведомлений о событиях
Создание сертификата для SMTP-сервера
Выборки событий
Просмотр выборки событий
Настройка параметров выборки событий

Создание выборки событий
Экспорт выборки событий в текстовый файл
Удаление событий из выборки
Добавление приложений в исключения по запросам пользователей
Выборки устройств
Просмотр выборки устройств
Настройка выборки устройств
Экспорт параметров выборки устройств в файл
Создание выборки устройств
Создание выборки устройств по импортированным параметрам
Удаление устройств из групп администрирования в выборке
Мониторинг установки и удаления приложений
События компонентов Kaspersky Security Center
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
События Сервера iOS MDM
События отказа функционирования Сервера iOS MDM
События предупреждения Сервера iOS MDM
Информационные события Сервера iOS MDM
Блокировка частых событий
О блокировке частых событий
Управление блокировкой частых событий
Отмена блокировки частых событий
Экспорт списка частых событий в файл
Контроль изменения состояния виртуальных машин
Отслеживание состояния антивирусной защиты с помощью информации в системном реестре
Просмотр и настройка действий, когда устройство неактивно
Выключение объявлений "Лаборатории Касперского"
Настройка точек распространения и шлюзов соединений
Типовая конфигурация точек распространения: один офис
Типовая конфигурация точек распространения: множество небольших удаленных офисов
Назначение управляемого устройства точкой распространения
Подключение устройства под управлением Linux в качестве шлюза в демилитаризованной зоне
Подключение устройства под управлением Linux к Серверу администрирования с помощью шлюза соединения
Добавление шлюза соединения в демилитаризованной зоне в качестве точки распространения
Автоматическое назначение точек распространения
О локальной установке Агента администрирования на устройство, выбранное точкой распространения
Об использовании точки распространения в качестве шлюза соединений

Добавление IP-диапазонов в список диапазонов, опрашиваемых точкой распространения
Использование точки распространения в качестве извещающего сервера
Другие повседневные задачи
Управление Серверами администрирования
Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования
Подключение к Серверу администрирования и переключение между Серверами администрирования
Права доступа к Серверу администрирования и его объектам
Условия подключения к Серверу администрирования через интернет
Защищенное подключение к Серверу администрирования
Аутентификация Сервера при подключении устройства
Аутентификация Сервера при подключении Консоли администрирования
Настройка списка разрешенных IP-адресов для подключения к Серверу администрирования
Использование утилиты klscflag для закрытия порта 13291
Отключение от Сервера администрирования
Добавление Сервера администрирования в дерево консоли
Удаление Сервера администрирования из дерева консоли
Добавление виртуального Сервера администрирования в дерево консоли
Смена учетной записи службы Сервера администрирования. Утилита klsrvswch
Изменение учетных данных СУБД
Изменение общей папки Сервера администрирования
Решение проблем с узлами Сервера администрирования
Просмотр и изменение параметров Сервера администрирования
Настройка общих параметров Сервера администрирования
Параметры интерфейса Консоли администрирования
Обработка и хранение событий на Сервере администрирования
Просмотр журнала подключений к Серверу администрирования
Контроль возникновения вирусных эпидемий
Ограничение трафика
Настройка параметров Веб-сервера
Работа с внутренними пользователями
Резервное копирование и восстановление параметров Сервера администрирования
Использование снимка файловой системы для уменьшения времени резервного копирования
Вышло из строя устройство с Сервером администрирования
Повреждены параметры Сервера администрирования или база данных
Резервное копирование и восстановление данных Сервера администрирования
Задача Резервное копирование данных Сервера администрирования
Утилита резервного копирования и восстановления данных (klbackup)
Резервное копирование и восстановление данных в интерактивном режиме
Резервное копирование и восстановление данных в тихом режиме
Использование утилиты klbackup для переключения управляемых устройств под управление другого Сервера администрирования
Резервное копирование и восстановление данных Сервера администрирования при использовании MySQL или MariaDB
Оптимизация процесса копирования и восстановления данных Сервера администрирования
Перенос Сервера администрирования на другое устройство
Избегание конфликтов между Серверами администрирования

Управление группами администрирования
Создание групп администрирования
Перемещение групп администрирования
Удаление групп администрирования
Автоматическое создание структуры групп администрирования
Автоматическая установка приложений на устройства группы администрирования
Управление клиентскими устройствами
Подключение клиентских устройств к Серверу администрирования
Подключение клиентского устройства к Серверу администрирования вручную. Утилита klmover
Туннелирование соединения клиентского устройства с Сервером администрирования
Удаленное подключение к рабочему столу клиентского устройства
Подключение к клиентским устройствам с операционной системой Windows
Подключение к клиентским устройствам с операционной системой macOS
Подключение к устройствам с помощью совместного доступа к рабочему столу Windows
Настройка перезагрузки клиентского устройства
Аудит действий на удаленном клиентском устройстве
Проверка соединения клиентского устройства с Сервером администрирования
Автоматическая проверка соединения клиентского устройства с Сервером администрирования
Проверка соединения клиентского устройства с Сервером администрирования вручную Утилита klnagchk
О проверке времени соединения устройства с Сервером администрирования
Идентификация клиентских устройств на Сервере администрирования
Перемещение устройств в состав группы администрирования
Смена Сервера администрирования для клиентских устройств
Перемещение устройств, подключенных к Серверу администрирования через шлюзы соединения, на другой Сервер администрирования
Кластеры и массивы серверов
Удаленное включение, выключение и перезагрузка клиентских устройств
Об использовании постоянного соединения между управляемым устройством и Сервером администрирования
О принудительной синхронизации
О расписании соединений
Отправка сообщения пользователям устройств
Работа с приложением Kaspersky Security для виртуальных сред
Настройка переключения статусов устройств
Назначение тегов устройствам и просмотр назначенных тегов
Автоматическое назначение тегов устройствам
Просмотр и настройка тегов, назначенных устройству
Удаленная диагностика клиентских устройств. Утилита удаленной диагностики Kaspersky Security Center
Подключение утилиты удаленной диагностики к клиентскому устройству
Создание файла дампа для приложения
Включение и выключение трассировки, загрузка файла трассировки
Загрузка параметров приложений
Загрузка журналов событий
Загрузка нескольких диагностических информационных элементов
Запуск диагностики и загрузка ее результатов
Запуск, остановка и перезапуск приложений
Устройства с защитой на уровне UEFI
Параметры управляемого устройства

Общие параметры политик
Параметры политики Агента администрирования
Управление учетными записями пользователей
Работа с учетными записями пользователей
Добавление учетной записи внутреннего пользователя
Изменение учетной записи внутреннего пользователя
Изменение количества попыток ввода пароля
Настройка проверки уникальности имени внутреннего пользователя
Добавление группы безопасности
Добавление пользователя в группу
Настройка прав доступа к функциям приложения. Управление доступом на основе ролей
Права доступа к функциям приложения
Предопределенные роли пользователей
Добавление роли пользователя
Назначение роли пользователю или группе безопасности
Назначение прав пользователям или группам пользователей
Распространение пользовательских ролей на подчиненные Серверы администрирования
Назначение пользователя владельцем устройства
Рассылка сообщений пользователям
Просмотр списка мобильных устройств пользователя
Установка сертификата пользователю
Просмотр списка сертификатов, выписанных пользователю
Об администраторе виртуального Сервера администрирования
Удаленная установка операционных систем и приложений
Создание образов операционных систем
Установка образов операционных систем
Настройка адреса прокси-сервера KSN
Добавление драйверов для среды предустановки Windows (WinPE)
Добавление драйверов в инсталляционный пакет с образом операционной системы
Настройка параметров утилиты sysprep.exe
Развертывание операционных систем на новых устройствах в сети
Развертывание операционных систем на клиентских устройствах
Создание инсталляционных пакетов приложений
Выписка сертификата для инсталляционных пакетов приложений
Установка приложений на клиентские устройства.
Работа с ревизиями объектов
О ревизиях объектов
Просмотр раздела История ревизий
Сравнение ревизий объекта
Установка срока хранения ревизий объектов и информации об удаленных объектах
Просмотр ревизии объекта
Сохранение ревизии объекта в файле
Откат изменений
Добавление описания ревизии

Удаление объектов
Удаление объекта
Просмотр информации об удаленных объектах
Удаление объектов из списка удаленных объектов
Управление мобильными устройствами
Сценарий: развертывание Управления мобильными устройствами
О групповых политиках для управления iOS MDM-устройствами
Включение Управления мобильными устройствами
Изменение параметров Управления мобильными устройствами
Выключение Управления мобильными устройствами
Работа с командами для мобильных устройств
Команды для управления мобильными устройствами
Использование Firebase Cloud Messaging
Отправка команд
Просмотр статусов команд в журнале команд
Работа с сертификатами для мобильных устройств
Запуск мастера установки сертификата
Шаг 1. Выбор типа сертификата
Шаг 2. Выбор типа устройства
Шаг 3. Выбор пользователя
Шаг 4. Выбор источника сертификата
Шаг 5. Назначение тега сертификатам
Шаг 6. Описание параметров публикации сертификата
Шаг 7. Выбор способа уведомления пользователей
Шаг 8. Генерация сертификата
Настройка правил выпуска сертификатов
Интеграция с инфраструктурой открытых ключей
Включение поддержки Kerberos Constrained Delegation
Добавление мобильных устройств iOS в список управляемых устройств
Добавление мобильных устройств Android в список управляемых устройств
Управление iOS MDM-устройствами
Подписание iOS MDM-профиля сертификатом
Добавление конфигурационного профиля
Установка конфигурационного профиля на устройство
Удаление конфигурационного профиля с устройства
Добавление нового устройства посредством публикации ссылки на профиль
Добавление нового устройства посредством установки профиля администратором
Добавление provisioning-профиля
Установка provisioning-профиля на устройство
Удаление provisioning-профиля с устройства
Добавление управляемого приложения
Установка приложения на мобильное устройство
Удаление приложения с устройства
Настройка параметров роуминга на мобильном устройстве iOS MDM
Просмотр информации о iOS MDM-устройстве
Отключение iOS MDM-устройства от управления

Отправка команд на устройство
Проверка статуса исполнения отправленных команд
Управление KES-устройствами
Создание пакета мобильных приложений для KES-устройств
Включение проверки подлинности на основе сертификатов KES-устройств
Просмотр информации о KES-устройстве
Отключение KES-устройства от управления
Шифрование и защита данных
Просмотр списка зашифрованных устройств
Просмотр списка событий шифрования
Экспорт списка событий шифрования в текстовый файл
Формирование и просмотр отчетов о шифровании
Передача ключей шифрования между Серверами администрирования
Хранилища данных
Экспорт списка объектов, находящихся в хранилище, в текстовый файл
Инсталляционные пакеты
Основные статусы файлов в хранилище
Срабатывание правил в режиме Интеллектуального обучения
Просмотр списка обнаружений, выполненных с помощью правил Адаптивного контроля аномалий
Добавление исключений в правила Адаптивного контроля аномалий
Шаг 1. Лицензирование приложения
Шаг 2. Выбор политики (политик)
Шаг 3. Обработка политики (политик)
Карантин и резервное хранилище
Включение удаленного управления файлами в хранилищах
Просмотр свойств файла, помещенного в хранилище
Удаление файлов из хранилища
Восстановление файлов из хранилища
Сохранение файла из хранилища на диск
Сканирование файлов, находящихся на карантине
Активные угрозы
Дезинфекция необработанного файла
Сохранение необработанного файла на диск
Удаление файлов из папки "Активные угрозы"
Kaspersky Security Network (KSN)
О KSN
Настройка доступа к Kaspersky Security Network
Включение и отключение KSN
Просмотр принятого Положения о KSN
Просмотр статистики прокси-сервера KSN
Принятие обновленного Положения о KSN
Дополнительная защита с использованием Kaspersky Security Network
Проверка, работает ли точка распространения как прокси-сервер KSN
Переключение между онлайн-справкой и офлайн-справкой
Export of events to SIEM systems
Настройка экспорта событий в SIEM-системы
Предварительные условия

О событиях в Kaspersky Security Center
Об экспорте событий
О настройке 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
Об экспорте событий в форматах CEF и LEEF
Настройка Kaspersky Security Center для экспорта событий в SIEM-систему
Экспорт событий напрямую из базы данных
Выполнение SQL-запроса с помощью утилиты klsql2
Пример SQL-запроса, созданного с помощью утилиты klsql2
Просмотр имени базы данных Kaspersky Security Center
Просмотр результатов экспорта
Использование SNMP для отправки статистики приложениям сторонних производителей
Настройка SNMP-службы для использования с Kaspersky Security Center
SNMP-агент и идентификаторы объектов
Получение имени счетчика строк из идентификатора объекта
Значения идентификаторов объектов для SNMP
Устранение неисправностей
Работа в облачном окружении
О работе в облачном окружении
Сценарий: развертывание в облачном окружении
Предварительные условия для развертывания Kaspersky Security Center в облачном окружении
Аппаратные требования для Сервера администрирования в облачном окружении
Варианты лицензирования в облачном окружении
Параметры базы данных для работы в облачном окружении
Работа в облачном окружении Amazon Web Services
О работе в облачном окружении Amazon Web Services
Создание IAM-роли и учетных записей IAM-пользователя для инстансов Amazon EC2
Обеспечение прав для работы Сервера администрирования Kaspersky Security Center с AWS
Создание IAM-роли для Сервера администрирования
Создание учетной записи IAM-пользователя для работы Kaspersky Security Center
Создание IAM-роли для установки приложений на инстансы Amazon EC2
Работа с Amazon RDS
Создание инстанса Amazon RDS
Создание группы параметров для инстанса Amazon RDS
Изменение группы параметров
Изменение прав IAM-роли для инстанса базы данных Amazon RDS
Подготовка корзины Amazon S3 для базы данных
Перенос базы данных в Amazon RDS
Работа в облачном окружении Microsoft Azure
О работе в Microsoft Azure
Создание подписки, идентификатора приложения и пароля
Назначение роли для ID приложения в Azure
Развертывание Сервера администрирования в Microsoft Azure и выбор базы данных

Работа с Azure SQL
Создание учетной записи хранения Azure
Создание базы данных Azure SQL и SQL-сервера
Перенос базы данных в Azure SQL
Работа в Google Cloud
Создание электронной почты клиента, идентификатора проекта и закрытого ключа
Работа с экземпляром Google Cloud SQL для MySQL
Подготовка клиентских устройств в облачном окружении для работы с Kaspersky Security Center
Создание инсталляционных пакетов, необходимых для настройки облачного окружения
Настройка облачного окружения
О мастере настройки облачного окружения
Шаг 1. Выбор способа активации приложения
Шаг 2. Выбор облачного окружения
Шаг 3. Аутентификация в облачном окружении
Шаг 4. Настройка синхронизации с облачным окружением и определение дальнейших действий
Шаг 5. Настройка Kaspersky Security Network в облачном окружении
Шаг 6. Настройка параметров отправки уведомлений по электронной почте в облачном окружении
Шаг 7. Создание первоначальной конфигурации защиты в облачном окружении
Шаг 8. Выбор действия, когда требуется перезагрузка операционной системы в ходе установки (для облачного окружения)
Шаг 9. Получение обновлений Сервером администрирования
Проверка успешности настройки
Группа облачных устройств
Опрос облачного сегмента
Добавление соединений для опроса облачных сегментов
Удаление соединений для опроса облачных сегментов
Настройка расписания опроса
Установка приложений на устройства в облачном окружении
Просмотр свойств облачных устройств
Синхронизация с облачным окружением
Схема работы Kaspersky Security Center в Yandex.Cloud
Приложения
Дополнительные возможности
Автоматизация работы Kaspersky Security Center. Утилита klakaut
Работа с внешними инструментами
Режим клонирования диска Агента администрирования
Подготовка эталонного устройства с установленным Агентом администрирования для создания образа операционной системы
Настройка параметров получения сообщений от компонента Мониторинг файловых операций
Обслуживание Сервера администрирования
Доступ к общедоступным DNS-серверам
Окно Способ уведомления пользователей
Окно Выборка устройств
Окно Определение названия создаваемого объекта
Особенности работы с интерфейсом управления
Дерево консоли
Как обновить данные в рабочей области

Как перемещаться по дереву консоли

Как открыть окно свойств объекта в рабочей области

Как выбрать группу объектов в рабочей области

Как изменить набор граф в рабочей области

Справочная информация

Команды контекстного меню

Список управляемых устройств. Значение граф

Статусы устройств, задач и политик

Значки статусов файлов в Консоли администрирования

Поиск и экспорт данных

Поиск устройств

Параметры поиска устройств

Использование масок в строковых переменных

Использование регулярных выражений в строке поиска

Экспорт списков из диалоговых окон

Параметры задач

Общие параметры задач

Параметры задачи загрузки обновлений в хранилище Сервера администрирования

Параметры задачи загрузки обновлений в хранилища точек распространения

Параметры задачи поиска уязвимостей и требуемых обновлений.

Параметры задачи установки требуемых обновлений и закрытия уязвимостей

Глобальный список подсетей

Добавление подсети в глобальный список подсетей

Просмотр и изменение свойств подсети в глобальном списке подсетей

Использование Агента администрирования для Windows, Linux и macOS: сравнение

Kaspersky Security Center Web Console

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

Порты, используемые приложением Kaspersky Security Center Web Console

Интерфейс Kaspersky Security Center Web Console

Закрепление и отмена закрепления разделов главного меню

Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console

Установка

Установка Kaspersky Security Center (Стандартная установка)

Установка Kaspersky Security Center Web Console

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

Обновление Kaspersky Security Center Web Console

Сертификаты для работы с Kaspersky Security Center Web Console

Перевыпуск сертификата для Kaspersky Security Center Web Console

Замена сертификата для Kaspersky Security Center Web Console

Указание сертификатов для доверенных Серверов администрирования в Kaspersky Security Center Web Console

Преобразование сертификата из формата PFX в формат PEM

Перенос данных из Kaspersky Security Center Windows

Перенос данных в Kaspersky Security Center Cloud Console

Перенос данных в Kaspersky Symphony XDR

Перенос данных в приложение Kaspersky Security Center Linux
Перенос данных в Kaspersky Security Center Linux с использованием резервной копии данных Сервера администрирования
Перенос данных в Kaspersky Security Center Linux с помощью мастера переноса данных
Экспорт групповых объектов из Kaspersky Security Center Windows
Импорт файла экспорта в Kaspersky Security Center Linux
Переключение управляемых устройств под управление Kaspersky Security Center Linux
Вход в приложение Kaspersky Security Center Web Console и выход из него
Identity and Access Manager в Kaspersky Security Center Web Console
О компоненте Identity and Access Manager
Включение Identity and Access Manager: сценарий
Настройка Identity and Access Manager в Kaspersky Security Center Web Console
Регистрация приложения Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center Web Console
Время жизни токенов и время ожидания авторизации для Identity and Access Manager
Загрузка и распространение IAM-сертификатов
Отключение Identity and Access Manager
Настройка доменной аутентификации с использованием протоколов NTLM и Kerberos
Настройка Сервера администрирования
Настройка подключения Kaspersky Security Center Web Console к Серверу администрирования
Настройка журнала событий подключения к Серверу администрирования
Настройка параметров доступа Сервера администрирования к интернету
Настройка количества событий в хранилище событий
Параметры подключения устройств с защитой на уровне UEFI
Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования
Просмотр списка подчиненных Серверов администрирования
Удаление иерархии Серверов администрирования
Обслуживание Сервера администрирования
Настройка интерфейса
Управление виртуальными Серверами администрирования
Создание виртуального Сервера администрирования
Включение и выключение виртуального Сервера администрирования
Назначение администратора виртуального Сервера администрирования
Смена Сервера администрирования для клиентских устройств
Удаление виртуального Сервера администрирования
Включение защиты учетной записи от несанкционированного изменения
Резервное копирование и восстановление данных Сервера администрирования
Создание задачи резервного копирования данных
Перенос Сервера администрирования на другое устройство
Проверка целостности модулей с помощью утилит klscmodchk и integrity_checker
Первоначальная настройка Kaspersky Security Center Web Console
Мастер первоначальной настройки (Kaspersky Security Center Web Console)
Шаг 1. Указание параметров подключения к интернету
Шаг 2. Загрузка требуемых обновлений
Шаг 3. Выбор активов для защиты
Шаг 4. Выбор шифрования
Шаг 5. Настройка установки плагинов для управляемых приложений
Шаг 6. Установка выбранных плагинов

Шаг 7. Загрузка дистрибутивов и создание инсталляционных пакетов
Шаг 8. Настройка Kaspersky Security Network
Шаг 9. Выбор способа активации приложения
Шаг 10. Указание параметров управления обновлениями приложений сторонних производителей
Шаг 11. Создание базовой конфигурации защиты сети
Шаг 12. Настройка параметров отправки уведомлений по электронной почте
Шаг 13. Выполнение опроса сети
Шаг 14. Завершение работы мастера первоначальной настройки
Подключение автономных устройств
Сценарий: подключение автономных устройств через шлюз соединения
Сценарий: подключение автономных устройств через подчиненный Сервер администрирования в демилитаризованной зоне
О подключении автономных устройств
Подключение внешних настольных устройств к Серверу администрирования
О профилях соединения для автономных пользователей
Создание профиля соединения для автономных пользователей
О переключении Агента администрирования на другой Сервер администрирования
Создание правила переключения Агента администрирования по сетевому местоположению
Мастер развертывания защиты
Шаг 1. Запуск мастера развертывания защиты
Шаг 2. Выбор инсталляционного пакета
Шаг 3. Выбор способа распространения файла ключа или кода активации
Шаг 4. Выбор версии Агента администрирования
Шаг 5. Выбор устройств
Шаг 6. Задание параметров задачи удаленной установки
Шаг 7. Управление перезагрузкой
Шаг 8. Удаление несовместимых приложений перед установкой
Шаг 9. Перемещение устройств в папку Управляемые устройства
Шаг 10. Выбор учетных записей для доступа к устройствам
Шаг 11. Запуск установки
Развертывание приложений "Лаборатории Касперского" с помощью Kaspersky Security Center Web Console
Сценарий: развертывание приложений "Лаборатории Касперского" с помощью Kaspersky Security Center Web Console
Загрузка плагинов для приложений "Лаборатории Касперского"
Загрузка и создание инсталляционных пакетов для приложений "Лаборатории Касперского"
Изменение ограничения на размер пользовательского инсталляционного пакета
Загрузка дистрибутивов для приложений "Лаборатории Касперского"
Проверка успешности развертывания Kaspersky Endpoint Security
Создание автономного инсталляционного пакета
Просмотр списка автономных инсталляционных пакетов
Создание пользовательского инсталляционного пакета
Распространение инсталляционных пакетов на подчиненные Серверы администрирования
Установка приложений с помощью задачи удаленной установки
Удаленная установка приложений
Установка приложения с помощью групповых политик Active Directory
Установка приложений на подчиненные Серверы администрирования
Указание параметров удаленной установки на устройствах под управлением Unix

- Запуск и остановка приложений "Лаборатории Касперского"
- Управление мобильными устройствами
- Замещение приложений безопасности сторонних производителей

Обнаружение устройств в сети

- Сценарий: обнаружение сетевых устройств
- Обнаружение устройств
  - Опрос сети Windows
  - Опрос IP-диапазонов
  - Добавление и изменение IP-диапазона
  - Опрос Zeroconf
  - Опрос контроллеров домена
  - Аутентификация и подключение к контроллеру домена
  - Настройка контроллеров домена Samba
  - Настройка правил хранения для нераспределенных устройств
  - Инвентаризация оборудования
    - Добавление информации о новых устройствах
    - Настройка критериев определения корпоративных устройств

Приложения "Лаборатории Касперского": лицензирование и активация

- Лицензирование управляемых приложений
- Добавление лицензионного ключа в хранилище Сервера администрирования
- Добавление лицензионного ключа Сервера администрирования
- Распространение лицензионного ключа на клиентские устройства
- Автоматическое распространение лицензионного ключа
- Просмотр информации об используемых лицензионных ключах
- Удаление лицензионного ключа из хранилища
- Отзыв согласия с Лицензионным соглашением
- Продление срока действия лицензии приложений "Лаборатории Касперского"
- Использование Kaspersky Marketplace для выбора бизнес-решений

Настройка 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
- Включение и выключение режима низкого потребления ресурсов для Агента администрирования
- Настройка параметров защиты управляемых приложений
- Ручная настройка групповой задачи обновления Kaspersky Endpoint Security
- Удаленная деинсталляция приложений или обновлений программного обеспечения
- Задачи
  - О задачах
  - Область задачи
  - Создание задачи
  - Запуск задачи вручную
  - Просмотр списка задач
  - Общие параметры задач
  - Экспорт задачи

Импорт задачи
Запуск мастера изменения паролей задач
Шаг 1. Выбор учетных данных
Шаг 2. Выбор выполняемого действия
Шаг 3. Просмотр результатов
Создание задачи Удаленное выполнение скриптов
Удаленная установка приложений на устройства с помощью задачи Удаленное выполнение скриптов
Настройка уведомлений и мониторинга для задачи Удаленное выполнение скриптов
Подготовка архива для задачи Удаленное выполнение скриптов
Создание инсталляционного пакета на основе манифест-файла
Управление клиентскими устройствами
Параметры управляемого устройства
Создание групп администрирования
Добавление устройств в состав группы администрирования вручную
Перемещение устройств или кластеров в состав группы администрирования вручную
Создание правил перемещения устройств
Копирование правил перемещения устройств
Условия для правила перемещения устройств
О кластерах и массивах серверов
Свойства кластеров или массивов серверов
Просмотр и настройка действий, когда устройство неактивно
О статусах устройства
Настройка переключения статусов устройств
Удаленное подключение к рабочему столу клиентского устройства
Подключение к устройствам с помощью совместного доступа к рабочему столу Windows
Выборки устройств
Просмотр списка устройств из выборки устройств
Создание выборки устройств
Настройка выборки устройств
Экспорт списка устройств из выборки устройств
Удаление устройств из групп администрирования в выборке
Теги устройств
Создание тегов устройств
Изменение тегов устройств
Удаление тегов устройств
Просмотр устройств, которым назначен тег
Просмотр тегов, назначенных устройству
Назначение тегов устройству вручную
Удаление назначенного тега с устройства
Просмотр правил автоматического назначения тегов устройствам
Изменение правил автоматического назначения тегов устройствам
Создание правил автоматического назначения тегов устройствам
Выполнение правил автоматического назначения тегов устройствам
Удаление правил автоматического назначения тегов с устройств
Управление тегами устройств с помощью утилиты klscflag

Политики и профили политик
- О политиках и профилях политик
- Блокировка (замок) и заблокированные параметры
- Наследование политик и профилей политик
  - Иерархия политик
  - Профили политик в иерархии политик
  - Как параметры реализованы на управляемом устройстве
- Управление политиками
  - Просмотр списка политик
  - Создание политики
  - Изменение политики
  - Общие параметры политик
  - Включение и выключение параметра наследования политики
  - Копирование политики
  - Перемещение политики
  - Экспорт политики
  - Импорт политики
  - Просмотр диаграммы состояния применения политики
  - 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

Шифрование и защита данных
- Просмотр списка зашифрованных жестких дисков
- Просмотр списка событий шифрования
- Формирование и просмотр отчетов о шифровании
- Предоставление доступа к зашифрованному жесткому диску в автономном режиме

Пользователи и роли пользователей
- О ролях пользователей
- Просмотр учетных записей и сеансов пользователей
- Настройка прав доступа к функциям приложения. Управление доступом на основе ролей
  - Права доступа к функциям приложения
  - Предопределенные роли пользователей
  - Назначение прав доступа к набору объектов
  - Назначение прав пользователям или группам безопасности
- Добавление учетной записи внутреннего пользователя
- Создание группы безопасности
- Изменение учетной записи внутреннего пользователя
- Изменение группы безопасности
- Назначение роли пользователю или группе безопасности
- Добавление учетных записей пользователей во внутреннюю группу безопасности
- Назначение пользователя владельцем устройства

Настройка двухфакторной аутентификации для всех пользователей
О двухфакторной аутентификации
Включение двухфакторной аутентификации для вашей учетной записи (Web Console)
Включение двухфакторной аутентификации для вашей учетной записи (на базе MMC)
Включение обязательной двухфакторной аутентификации для всех пользователей (Web Console)
Включение двухфакторной аутентификации для всех пользователей (на базе MMC)
Выключение двухфакторной аутентификации для учетной записи пользователя (Web Console)
Выключение двухфакторной аутентификации для учетной записи пользователя (на базе MMC)
Выключение обязательной двухфакторной аутентификации для всех пользователей (Web Console)
Выключение обязательной двухфакторной аутентификации для всех пользователей (на базе MMC)
Исключение учетных записей из двухфакторной аутентификации (Web Console)
Исключение учетных записей из двухфакторной аутентификации (на базе MMC)
Изменение имени издателя кода безопасности (Web Console)
Изменение имени издателя кода безопасности (на базе MMC)
Настройка двухфакторной аутентификации для вашей учетной записи (Web Console)
Настройка двухфакторной аутентификации для вашей учетной записи (на базе MMC)
Генерация нового секретного ключа
Запретить новым пользователям настраивать для себя двухэтапную проверку
Назначение пользователя владельцем устройства Linux после установки Агента администрирования
Удаление пользователей или групп безопасности
Изменение пароля учетной записи пользователя
Создание роли пользователя
Изменение роли пользователя
Изменение области для роли пользователя
Удаление роли пользователя
Связь профилей политики с ролями
Распространение пользовательских ролей на подчиненные Серверы администрирования
Смена пароля учетной записи
Отзыв прав локального администратора
Работа с ревизиями объектов
Откат изменений объекта к предыдущей ревизии
Добавление описания ревизии
Просмотр и сохранение ревизии политики
Удаление объектов
Kaspersky Security Network (KSN)
О KSN
Настройка доступа к KSN
Включение и выключение использования KSN
Просмотр принятого Положения о KSN
Принятие обновленного Положения о KSN
Проверка, работает ли точка распространения как прокси-сервер KSN
Сценарий: обновление Kaspersky Security Center и управляемых приложений безопасности
Обновление баз и приложений "Лаборатории Касперского"
Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"
Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"
Создание задачи Загрузка обновлений в хранилище Сервера администрирования
Проверка полученных обновлений

Создание задачи загрузки обновлений в хранилища точек распространения
Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center
Автоматическая установка обновлений для Kaspersky Endpoint Security для Windows
Одобрение и отклонение обновлений программного обеспечения
Обновление Сервера администрирования
Включение и выключение офлайн-модели получения обновлений
Обновление баз и модулей приложений "Лаборатории Касперского" на автономных устройствах
Резервное копирование и восстановление веб-плагинов
Настройка точек распространения и шлюзов соединений
Типовая конфигурация точек распространения: один офис
Типовая конфигурация точек распространения: множество небольших удаленных офисов
О назначении точек распространения
Автоматическое назначение точек распространения
Назначение точек распространения вручную
Изменение списка точек распространения для группы администрирования
Принудительная синхронизация
Включение push-сервера
Управление приложениями сторонних производителей на клиентских устройствах
Установка обновлений 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.
Создание задачи Синхронизация обновлений Windows Update
Автоматическое обновление приложений сторонних производителей
Закрытие уязвимостей в приложениях сторонних производителей
Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей
Об обнаружении и закрытии уязвимостей в приложениях
Закрытие уязвимостей в приложениях сторонних производителей
Создание задачи Закрытие уязвимостей
Создание задачи Установка требуемых обновлений и закрытие уязвимостей
Добавление правил для установки обновлений
Пользовательские исправления для уязвимостей в приложениях сторонних производителей
Просмотр информации об уязвимостях в приложениях, обнаруженных на всех управляемых устройствах
Просмотр информации об уязвимостях в приложениях, обнаруженных на выбранных управляемых устройствах
Просмотр статистики уязвимостей на управляемых устройствах.
Экспорт списка уязвимостей в приложениях в текстовый файл
Игнорирование уязвимостей в приложениях

Управление запуском приложений на клиентских устройствах
Использование компонента Контроль приложений для управления исполняемыми файлами
Режимы и категории компонента Контроль приложений
Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах
Создание пополняемой вручную категории приложений
Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств
Создание категории приложений, в которую входят исполняемые файлы из выбранных папок
Просмотр списка категорий приложений
Добавление исполняемых файлов, связанных с событием, в категорию приложения
Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows
Получение и просмотр списка приложений, установленных на клиентских устройствах
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
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 Kaspersky Security Center
Использование выборок событий
Создание выборки событий
Изменение выборки событий

Просмотр списка выборки событий
Экспорт выборки событий
Импорт выборки событий
Просмотр информации о событии
Экспорт событий в файл
Просмотр истории объекта из события
Удаление событий
Удаление выборок событий
Настройка срока хранения события
События компонентов Kaspersky Security Center
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
События Сервера iOS MDM
События отказа функционирования Сервера iOS MDM
События предупреждения Сервера iOS MDM
Информационные события Сервера iOS MDM
Блокировка частых событий
О блокировке частых событий
Управление блокировкой частых событий
Отмена блокировки частых событий
Уведомления и статусы устройств
Использование уведомлений
Просмотр экранных уведомлений
О статусах устройства
Настройка переключения статусов устройств
Настройка параметров доставки уведомлений
Уведомление о событиях с помощью исполняемого файла
Объявления "Лаборатории Касперского"
Об объявлениях "Лаборатории Касперского"
Настройка параметров объявлений "Лаборатории Касперского"
Выключение объявлений "Лаборатории Касперского"
Просмотр информации об обнаруженных угрозах
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
Журнал активности Kaspersky Security Center Web Console

Интеграция Kaspersky Security Center с другими решениями
Установка фонового соединения
Экспорт событий в SIEM-системы
Настройка экспорта событий в SIEM-системы
Предварительные условия
О событиях в Kaspersky Security Center
Об экспорте событий
О настройке экспорта событий в SIEM-системе
Выбор событий для экспорта в SIEM-системы в формате syslog
О выборе событий для экспорта в SIEM-систему 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 форматах CEF и LEEF
Конвертация событий в формат CEF или LEEF
Об экспорте событий в формате Syslog
Настройка Kaspersky Security Center для экспорта событий в SIEM-систему
Экспорт событий напрямую из базы данных
Выполнение SQL-запроса с помощью утилиты klsql2
Пример SQL-запроса, созданного с помощью утилиты klsql2
Просмотр имени базы данных Kaspersky Security Center
Просмотр результатов экспорта
Работа с Kaspersky Security Center Web Console в облачном окружении
Настройка облачного окружения в Kaspersky Security Center Web Console
Шаг 1. Проверка требуемых плагинов и инсталляционных пакетов
Шаг 2. Лицензирование приложения
Шаг 3. Выбор облачного окружения и аутентификация
Шаг 4. Опрос сегмента, настройка синхронизации с облачным окружением и определение дальнейших действий
Шаг 5. Выбор приложения для создания политики и задач
Шаг 6. Настройка Kaspersky Security Network для Kaspersky Security Center
Шаг 7. Создание первоначальной конфигурации защиты
Опрос сегмента сети с помощью Kaspersky Security Center Web Console
Добавление соединений для опроса облачных сегментов
Удаление соединения для опроса облачных сегментов
Настройка расписания опроса с помощью Kaspersky Security Center Web Console
Просмотр результатов опроса облачного сегмента с помощью Kaspersky Security Center Web Console
Просмотр свойств облачных устройств с помощью Kaspersky Security Center Web Console
Синхронизация с облачным сегментом: настройка правила перемещения
Удаленная установка приложений на виртуальные машины Azure
Создание задачи резервного копирования данных Сервера администрирования с использованием облачной СУБД
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 журналов событий
Запуск, остановка и перезапуск приложения

Запуск удаленной диагностики Агента администрирования Kaspersky Security Center и скачивание результатов
Запуск приложения на клиентском устройстве
Создание файла дампа для приложения
Запуск удаленной диагностики на клиентском устройстве с операционной системой Linux
Загрузка и удаление файлов из разделов Карантин и Резервное хранилище
Загрузка файлов из разделов Карантин и Резервное хранилище
Изменение языка интерфейса Kaspersky Security Center Web Console
Справочное руководство API
Лучшие практики для поставщиков услуг
Планирование развертывания Kaspersky Security Center
Предоставление доступа к Серверу администрирования из интернета
Типовая конфигурация Kaspersky Security Center
О точках распространения
Иерархия Серверов администрирования
Виртуальные Серверы администрирования
Управление мобильными устройствами с установленным Kaspersky Endpoint Security для Android
Развертывание и первоначальная настройка
Рекомендации по установке Сервера администрирования
Создание учетных записей для служб Сервера администрирования на отказоустойчивом кластере
Выбор СУБД
Указание адреса Сервера администрирования
Настройка защиты в сети организации-клиента
Ручная настройка политики Kaspersky Endpoint Security
Настройка политики в разделе Продвинутая защита
Настройка политики в разделе Базовая защита
Настройка политики в разделе Дополнительные параметры
Настройка политики в разделе Настройка событий
Ручная настройка групповой задачи обновления Kaspersky Endpoint Security
Ручная настройка групповой задачи проверки устройства Kaspersky Endpoint Security
Настройка расписания задачи Поиск уязвимостей и требуемых обновлений.
Ручная настройка групповой задачи установки обновлений и закрытия уязвимостей
Построение структуры групп администрирования и назначение точек распространения
Типовая конфигурация MSP-клиента: один офис
Типовая конфигурация MSP-клиента: множество небольших изолированных офисов
Иерархия политик, использование профилей политик
Иерархия политик
Профили политик
Tasks
Правила перемещения устройств
Категоризация программного обеспечения
О мультитенантных приложениях
Резервное копирование и восстановление параметров Сервера администрирования
Вышло из строя устройство с Сервером администрирования
Повреждены параметры Сервера администрирования или база данных

Развертывание Агента администрирования и приложения безопасности
Первоначальное развертывание
Настройка параметров инсталляторов
Инсталляционные пакеты
Свойства MSI и файлы трансформации
Развертывание при помощи сторонних средств удаленной установки приложений
Общие сведения о задачах удаленной установки приложений Kaspersky Security Center
Развертывание с помощью механизма групповых политик Microsoft Windows
Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center
Запуск автономных пакетов, сформированных Kaspersky Security Center
Возможности ручной установки приложений
Удаленная установка приложений на устройства с установленным Агентом администрирования
Управление перезагрузкой устройств в задаче удаленной установки
Целесообразность обновления баз в инсталляционном пакете антивирусного приложения
Удаление несовместимых приложений безопасности сторонних производителей
Удаление Агента администрирования, защищенного паролем, с помощью командной строки
Использование средств удаленной установки приложений Kaspersky Security Center для запуска на управляемых устройствах произвольных исполняемых файлов
Мониторинг развертывания
Настройка параметров инсталляторов
Общая информация
Установка в тихом режиме (с файлом ответов)
Установка Агента администрирования в тихом режиме (без файла ответов)
Частичная настройка параметров установки через setup.exe
Параметры установки Сервера администрирования
Параметры установки Агента администрирования
Виртуальная инфраструктура
Рекомендации по снижению нагрузки на виртуальные машины
Поддержка динамических виртуальных машин
Поддержка копирования виртуальных машин
Поддержка отката файловой системы для устройств с Агентом администрирования
О профилях соединения для автономных пользователей
Развертывание поддержки Управления мобильными устройствами
Подключение KES-устройств к Серверу администрирования
Прямое подключение устройств к Серверу администрирования
Схема подключения KES-устройств к Серверу с использованием принудительного делегирования Kerberos (KCD)
Использование Firebase Cloud Messaging
Интеграция с инфраструктурой открытых ключей
Веб-сервер Kaspersky Security Center
Другие повседневные задачи
Мониторинг цветовых индикаторов и зарегистрированных событий в Консоли администрирования
Удаленный доступ к управляемым устройствам
Использование параметра "Не разрывать соединение с Сервером администрирования" для обеспечения постоянной связи между управляемым устройством и Сервером администрирования
О проверке времени соединения устройства с Сервером администрирования

О принудительной синхронизации
О туннелировании
Руководство по масштабированию
Об этом руководстве
Информация об ограничениях Kaspersky Security Center
Расчеты для Серверов администрирования
Расчет аппаратных ресурсов для Сервера администрирования
Аппаратные требования для СУБД и Сервера администрирования
Расчет места в базе данных
Расчет места на диске (с учетом и без учета использования Системного администрирования)
Расчет количества и конфигурации Серверов администрирования
Рекомендации по подключению динамических виртуальных машин к Kaspersky Security Center
Расчеты для точек распространения и шлюзов соединений
Требования для точки распространения
Расчет количества и конфигурации точек распространения
Расчет количества шлюзов соединений
Хранение информации о событиях для задач и политик
Особенности и оптимальные параметры некоторых задач
Частота обнаружения устройств
Задачи резервного копирования данных Сервера администрирования и обслуживания Сервера администрирования
Групповые задачи обновления Kaspersky Endpoint Security
Задача Инвентаризации
Информация о нагрузке на сеть между Сервером администрирования и защищаемыми устройствами
Потребление трафика выполнении различных сценариев
Средний расход трафика за сутки
Обращение в Службу технической поддержки
Способы получения технической поддержки
Техническая поддержка через Kaspersky CompanyAccount
Получение файлов дампа Сервера администрирования
Источники информации о приложении
Глоссарий
AWS Application Program Interface (AWS API)
Cloud discovery
FileTransferBridge
HTTPS
IAM-пользователь
IAM-роль
Identity and Access Management (IAM)
iOS MDM-профиль
iOS MDM-устройство
JavaScript
Kaspersky Security Center System Health Validator (SHV)
Kaspersky Security Network (KSN)
KES-устройство
Lightweight Nagent (LWNGT)
MITM-атака
Network Location Awareness (NLA)

Provisioning-профиль

SSL

Windows Server Update Services (WSUS)

Агент администрирования

Агент аутентификации

Агент обновлений

Административные права

Администратор Kaspersky Security Center

Администратор клиента

Администратор поставщика услуг

Активный ключ

Антивирусная безопасность сети

Антивирусные базы

Веб-сервер Kaspersky Security Center

Виртуальный Сервер администрирования

Вирусная атака

Владелец устройства

Внутренние пользователи

Восстановление

Восстановление данных Сервера администрирования

Группа администрирования

Группа лицензионных программ

Групповая задача

Демилитаризованная зона (DMZ)

Домашний Сервер администрирования

Дополнительный ключ

Доступное обновление

Задача

Задача для набора устройств

Инсталляционный пакет

Инстанс Amazon EC2

Клиент Сервера администрирования (Клиентское устройство)

Ключ доступа IAM AWS

Консоль AWS

Консоль администрирования

Конфигурационный профиль

Локальная задача

Локальная установка

Магазин приложений

Настройки задачи

Непосредственное управление приложением

Несовместимое приложение

Облачное окружение

Обновление

Обновление приложения Kaspersky Security Center

Образ AMI

Общий сертификат

Оператор Kaspersky Security Center
Параметры приложения
Плагин управления приложением
Политика
Порог вирусной активности
Поставщик услуг антивирусной защиты
Рабочее место администратора
Резервное копирование данных Сервера администрирования
Руководство по усилению защиты
Ручная установка
Сервер iOS MDM
Сервер администрирования
Сервер мобильных устройств
Серверы обновлений "Лаборатории Касперского"
Сертификат Сервера администрирования
Состояние защиты
Состояние защиты сети
Срок действия лицензии
Удаленная установка
Управляемые устройства
Уровень важности патча
Уровень важности события
Устройство с защитой на уровне UEFI
Уязвимость
Файл ключа
Форсированная установка
Хранилище резервных копий
Хранилище событий
Централизованное управление приложением
Широковещательный домен
Шлюз соединения
Информация о стороннем коде
Уведомления о товарных знаках
Известные проблемы и ограничения

Справка Kaspersky Security Center 15.1

	**Что нового** Узнайте, что нового в этой версии приложения.		**Настройка защиты сети** Управление безопасностью организации.
	**Аппаратные и программные требования** Проверьте поддерживаемые операционные системы и версии приложений.		**Приложения "Лаборатории Касперского". Обновление баз и модулей приложений** Поддержка надежности системы защиты.
	**Развертывание и первоначальная настройка** Планирование ресурсов: установка Сервера администрирования, установка Агента администрирования и приложений безопасности на клиентских устройствах, объединение устройств в группы администрирования.		**Мониторинг и отчеты** Просмотр данных об инфраструктуре вашей сети, статусе защиты и статистики. Управление доступом к облачным службам с помощью Cloud Discovery.
	**Обнаружение устройств в сети** Обнаружение существующих и новых устройств в сети вашей организации.		**Замещение приложений безопасности сторонних производителей** Узнайте о методах удаления несовместимых приложений.
	**Приложения "Лаборатории Касперского". Централизованное развертывание** Развертывание приложений "Лаборатории Касперского".		**Настройка точек распространения и шлюзов соединений** Настройка точек распространения.
	**Обновление предыдущей версии Kaspersky Security Center** Обновление Kaspersky Security Center 15.1 из предыдущей версии.		**Лучшие практики для поставщиков услуг (только онлайн-справка)** Ознакомьтесь с рекомендациями по развертыванию, настройке и использованию приложения, а также со способами решения типичных проблем, возникающих при работе приложения.
	**Приложения "Лаборатории Касперского". Лицензирование и активация** Активация приложений "Лаборатории Касперского" в несколько шагов.		**Руководство по масштабированию (только онлайн-справка)** Для оптимальной производительности при различных условиях учитывайте количество устройств в сети, топологию сети и необходимый вам набор функций Kaspersky Security Center.
	**Экспорт событий в SIEM-системы** Настройте экспорт событий в SIEM-системы для анализа.		**Системное администрирование.** Обнаружение и закрытие уязвимостей в приложениях сторонних производителей.
	**Работа в облачном окружении** Развертывание Kaspersky Security Center в облачном окружении: Amazon Web Services™, Microsoft Azure™, Google™ платформа Google Cloud.		**Часто задаваемые вопросы (только на английском языке)** Найдите инструкции по устранению распространенных проблем.
	**Краткое руководство по началу работы с Kaspersky Endpoint Security для бизнеса** Начните работу с Kaspersky Endpoint Security для бизнеса: установите и настройте это решение. Вы также можете просмотреть сравнение функций Kaspersky Security Center, чтобы выбрать наиболее подходящий способ управления безопасностью сети.		

Что нового

Kaspersky Security Center 15.1 обновление 3

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

- Kaspersky Security Center 15.1 теперь поддерживает Kaspersky Password Manager для бизнеса.
- Сервер администрирования теперь поддерживает новые версии СУБД:
  - Microsoft SQL Server 2025.
  - MariaDB 11.4.
  - MariaDB 11.8.
  - MariaDB 12.3.
  - Postgres Pro 16.x.
  - Postgres Pro 17.x.
  - Postgres Pro 18.x.

Kaspersky Security Center 15.1 обновление 2

Kaspersky Security Center 15.1 обновление 2 направлено на устранение проблем, о которых сообщали пользователи и группа тестирования:

- Задачи теперь выполняются правильно для управляемых устройств под управлением Linux, указанных при импорте файла TXT.
- Теперь при установке приложения "Лаборатория Касперского" с помощью задачи удаленной установки, созданной на виртуальном Сервере администрирования, инсталляционные пакеты передаются на управляемые устройства средствами операционной системы только через точку распространения, управляемую этим виртуальным Сервером администрирования.
- Решена проблема, из-за которой подчиненный Сервер администрирования не мог повторно подключиться к главному Серверу администрирования после перевыпуска сертификата подчиненного Сервера.
- Решены проблемы, влияющие на TLS-подключения.
- Решена проблема, из-за которой при входе пользователя в приложение возникало несколько ошибок "Неверное преобразование типа".
- Kaspersky Security Center теперь правильно отправляет уведомления о событиях по электронной почте.

- Исправлена проблема с добавлением папки *Обновления* в резервную копию при обновлении Kaspersky Security Center с версии 14.2 до версии 15.1.
- Теперь в Kaspersky Security Center Web Console срок действия лицензии приложений "Лаборатории Касперского" отображается правильно.
- Теперь команды **Получить местоположение мобильного устройства** и **Получить историю местоположений** работают правильно.
- Исправлена ошибка, из-за которой инсталляционные пакеты с мобильными сертификатами не удалялись автоматически через один час после загрузки или через 24 часа после того, как они оставались неиспользованными.
- Профиль политики, активированный заданным тегом, теперь правильно применяется к устройствам, описания которых содержат этот тег.
- Исправлена проблема, из-за которой сообщения об ошибках базы данных PostgreSQL отображались в журнале событий.
- Исключение учетной записи из двухфакторной аутентификации теперь работает правильно.
- Исправлена ошибка, из-за которой выход из Kaspersky Security Center Web Console не работал должным образом при использовании доменной аутентификации с включенным Identity and Access Manager.
- Теперь при обновлении веб-плагина управления переход по ссылке с нужной версией плагина запускает загрузку.
- Исправленные проблемы в отчетах:
  - При создании задачи рассылки отчетов об угрозах и обновлениях и установки расписания задачи **Ежемесячно**, отчеты заполняются данными правильно.
  - В шаблоне *Отчет о статусе компонентов приложения* фильтры по имени компонента применяются правильно.
  - *Отчет о развертывании защиты* теперь можно отфильтровать, чтобы отображались только устройства, на которых не установлены приложения "Лаборатории Касперского". Это помогает визуализировать количество устройств, на которых будут установлены приложения.
- Виджет **Cloud Discovery** отображается правильно независимо от того, есть ли у вас право **Выполнение** в области **Общие функции: Базовая функциональность**.
- Повышена производительность хранимых процедур и операций с базами данных.
- Исправлена проблема, из-за которой сертификаты, с истекшим сроком действия и связанные с несуществующими пользователями, приводили к остановке процесса обновления для всех пользователей.
- Решены проблемы, влияющие на работу с сертификатами.
- Теперь после обновления Kaspersky Security Center с версии 14.2 до 15.1 загрузка автономного инсталляционного пакета с подчиненного виртуального Сервера администрирования в Консоли администрирования работает правильно.

- Исправлена проблема в Kaspersky Security Center Web Console, когда при включении использования Kaspersky Security Network (KSN) в политике приложений "Лаборатории Касперского", принятие Положения о KSN было недоступно для следующих приложений: Kaspersky Endpoint Security для Linux версии 12.2 и ниже, Kaspersky Industrial CyberSecurity for Linux Nodes версии 1.5 и ниже, Kaspersky Security для виртуальных сред Легкий агент версии 6.0 и 6.1, Kaspersky Embedded Systems Security для Linux версии 3.3 и Kaspersky Security для Windows Server версии 11.0.1.897.

- Исправлена проблема, из-за которой профиль политики не применялся к устройствам под управлением Linux, включенным в группу домена Active Directory.

- Исправлена проблема, возникавшая при попытках подключения нескольких подчиненных Серверов администрирования второго уровня к главному Серверу администрирования.

Kaspersky Security Center 15.1

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

- Cloud Discovery. Новая функциональность позволяет отслеживать использование облачных сервисов на управляемых устройствах с операционной системой Windows и блокировать доступ к нежелательным облачным сервисам. Эта функция доступна только в Kaspersky Security Center Web Console.

- Опрос контроллеров домена теперь позволяет опрашивать контроллеры домена Samba с помощью точки распространения с операционной системой Linux. Дополнительные доработки для поддержки опроса больших доменов.

- Расширенная удаленная диагностика управляемых устройств с операционной системой Linux.

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

- Теперь вы можете проверить подключение к SIEM-системе.

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

- Теперь при переносе данных из Kaspersky Security Center Windows в Kaspersky Security Center Linux вы можете переключить управляемые устройства под управление Kaspersky Security Center Linux с помощью восстановления сертификата и закрытого ключа Сервера администрирования из резервной копии данных.

- При запуске утилиты Cleaner или klmover для удаления Агента администрирования, защищенного паролем, вам будет предложено ввести пароль для удаления.

- Обновление с Kaspersky Security для Windows Server до Kaspersky Endpoint Security для Windows больше не требует перезагрузки целевого устройства.

- Пользователь может быть назначен владельцем устройства во время или после установки Агента администрирования на клиентском устройстве под управлением Linux.

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

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

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

- Улучшен пользовательский опыт при использовании приложения, в том числе:

  - Персонализация главного меню путем закрепления разделов Kaspersky Security Center Web Console для быстрого доступа из раздела **Закрепленное**.

  - Оптимизирована работа с таблицами. Представление по умолчанию для каждой таблицы теперь содержит наиболее часто используемые столбцы. Также теперь вы можете выбрать все элементы на текущей странице или во всей таблице и отсортировать элементы по всей таблице.

  - Улучшена конфигурация рассылки отчетов. Теперь вы можете указать до 20 адресов электронной почты для рассылки отчета и задать расписание рассылки отчета.

- Вы можете отозвать права локального администратора учетных записей на управляемых устройствах с операционной системой Linux. Это дает вам дополнительный уровень контроля учетных записей пользователей. Например, вы можете отозвать права локального администратора после завершения разового назначения.

- Вы можете изменить пароль локальной учетной записи на управляемых устройствах с операционной системой Linux, например, когда пользователь забыл пароль локальной учетной записи или чтобы изменить пароль по расписанию.

- В подразделе **Управление пользовательскими сертификатами** вы можете указать, какие корневые сертификаты устанавливать. Эти сертификаты могут использоваться, например, для проверки подлинности веб-сайтов или веб-серверов.

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

- Новый параметр, требующий изменения пароля при следующей попытке входа в Kaspersky Security Center Web Console внутреннего пользователя.

- Коммерческая лицензия больше не проверяется при экспорте событий в SIEM-систему в форматах CEF или LEEF.

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

- Exchange ActiveSync больше не поддерживается.

Kaspersky Security Center 14.2

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

- Выпущено Руководство по усилению защиты. Настоятельно рекомендуется внимательно прочитать руководство и следовать рекомендациям по безопасности при настройке Kaspersky Security Center и вашей сетевой инфраструктуры.

  Также установите последнее обновление Kaspersky Security Center. Это обновление включает функции защиты инфраструктуры, такие как двухфакторная аутентификация учетных записей пользователей и другие улучшения.

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

- Права пользователя виртуального Сервера администрирования настраиваются независимо от прав пользователей главного Сервера администрирования. Также вы можете предоставить пользователям главного Сервера права на управление виртуальным Сервером.

- Kaspersky Security Center теперь поддерживает работу со следующими СУБД:

  - PostgreSQL 13.x.
  - PostgreSQL 14.x.
  - Postgres Pro 13.x (все редакции).
  - Postgres Pro 14.x (все редакции).
  - MariaDB 10.1, 10.4, 10.5.

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

- Параметр **Не использовать прокси-сервер** удален из следующих задач:

  - *Загрузка обновлений в хранилище Сервера администрирования*
  - *Загрузка обновлений в хранилища точек распространения*

- Чтобы защитить клиентские устройства в облачном окружении, можно развернуть Kaspersky Endpoint Security для Windows вместо Kaspersky Security для Windows Server. Эта функция станет доступна после выхода новой версии Kaspersky Endpoint Security 12.0 для Windows.

- Работа с ключами шифрования теперь ограничена правами доступа в функциональной области **Общие функции**: **Управление ключами шифрования**. Пользователи Kaspersky Security Center теперь могут экспортировать ключи шифрования, если у них есть право **Чтение**, а также могут импортировать ключи шифрования, если у них есть право **Запись**.

Kaspersky Security Center 14

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

- Вы можете устанавливать обновления и закрывать уязвимости приложений сторонних производителей (кроме приложений Microsoft) в изолированной сети. К таким сетям относятся Серверы администрирования и управляемые устройства, не имеющие доступа в интернет. Для закрытия уязвимостей в такой сети необходимо загрузить необходимые обновления с помощью Сервера администрирования с доступом в интернет, а затем передать патчи на изолированные Серверы администрирования.

- Для устройств macOS добавлены профили подключения для автономных пользователей. С помощью профилей подключения вы можете настроить правила подключения Агентов администрирования на устройствах macOS к одному и тому же или к разным Серверам администрирования в зависимости от расположения устройства.

- Теперь Агент администрирования можно устанавливать на устройства с Microsoft Windows 10 IoT Enterprise.

- В отчете **Отчет об угрозах** теперь можно отфильтровать список угроз, чтобы просмотреть только те угрозы, которые были обнаружены Cloud Sandbox.

- Kaspersky Security Center теперь поддерживает Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 как управляемое приложение.

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

- Вы можете настраивать режим Просмотра только панели мониторинга для сотрудников, которые не управляют сетью, но хотят просматривать статистику защиты сети в Kaspersky Security Center (например, это может быть топ-менеджер). Когда у пользователя включен этот режим, 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.

- Kaspersky Security Center Web Console поддерживает Kaspersky Security для iOS как приложение безопасности.

- В свойствах задачи вы можете указать, хотите ли вы применять задачу к подгруппам и подчиненным Серверам администрирования (в том числе к виртуальным).

- Kaspersky Security Center теперь поддерживает Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 как управляемое приложение.

Kaspersky Security Center 13.2

В приложении Kaspersky Security Center 13.2 реализовано несколько новых функций и улучшений:

- Теперь вы можете установить Сервер администрирования, Консоль администрирования, Kaspersky Security Center 13.2 Web Console и Агент администрирования для следующих новых операционных системах (см. требования к программному обеспечению):
  - Microsoft Windows 11
  - Microsoft Windows 10 21H2 (October 2021 Update)
  - Windows Server 2022
- Вы можете использовать базу данных MySQL 8.0.
- Вы можете развернуть Kaspersky Security Center на отказоустойчивом кластере Kaspersky Security Center для обеспечения высокой доступности Kaspersky Security Center.
- Kaspersky Security Center теперь работает как с IPv6-адресами, так и с IPv4-адресами. Сервер администрирования может опрашивать сети, в которых есть устройства с IPv6-адресами.

В приложении Kaspersky Security Center 13.2 Web Console реализовано несколько новых функций и улучшений:

- Теперь вы можете управлять мобильными устройствами с операционной системой Android с помощью Kaspersky Security Center 13.2 Web Console.
- Kaspersky Marketplace доступен в виде нового раздела меню: вы можете искать приложения "Лаборатории Касперского" через Kaspersky Security Center 13.2 Web Console.
- Kaspersky Security Center теперь поддерживает следующие приложения "Лаборатории Касперского":
  - Kaspersky Endpoint Detection and Response Optimum 2.0.
  - Kaspersky Sandbox 2.0.
  - Kaspersky Industrial CyberSecurity for Networks 3.1.

Kaspersky Security Center 13.1

В приложении Kaspersky Security Center 13.1 реализовано несколько новых функций и улучшений:

- Улучшена интеграция с SIEM-системами. Теперь вы можете экспортировать события в SIEM-системы по зашифрованному каналу (TLS). Функция доступна для Kaspersky Security Center Web Console и для Консоли администрирования на основе консоли Microsoft Management Console (MMC).
- Теперь вы можете получать исправления для Сервера администрирования в виде дистрибутива, который можно использовать для будущих обновлений до более поздних версий.

- Добавлен раздел **Обнаружения** для Kaspersky Endpoint Detection and Response Optimum в Kaspersky Security Center 13.1 Web Console. Также добавлено несколько виджетов для работы с угрозами, обнаруженными Kaspersky Endpoint Detection and Response Optimum.

- В Kaspersky Security Center 13.1 Web Console вы можете получать уведомления об истечении срока действия лицензий для приложений "Лаборатории Касперского".

- Уменьшено время отклика Kaspersky Security Center 13.1 Web Console.

Kaspersky Security Center 13

В приложении Kaspersky Security Center 13 Web Console были реализованы следующие функции:

- Внедрена двухфакторная аутентификация. Вы можете включить двухфакторную аутентификацию, чтобы снизить риск несанкционированного доступа к Kaspersky Security Center 13 Web Console.

- Внедрена доменная аутентификации с использованием протоколов NTLM и Kerberos (единый вход). Функция единого входа позволяет пользователю Windows включить безопасную аутентификацию в Kaspersky Security Center 13 Web Console без повторного ввода пароля в корпоративной сети.

- Теперь вы можете настроить плагин для работы с Kaspersky Managed Detection and Response. Вы можете использовать эту интеграцию для просмотра инцидентов и управления рабочими станциями.

- Теперь вы можете указывать параметры Kaspersky Security Center 13 Web Console в мастере установки Сервера администрирования.

- Отображаются уведомления о новых выпусках обновлений и патчей. Вы можете установить обновление сразу или позже в любое время. Теперь вы можете устанавливать патчи для Сервера администрирования с помощью Kaspersky Security Center 13 Web Console.

- При работе с таблицами теперь можно указывать порядок и ширину граф, сортировать данные и указывать размер страницы.

- Вы можете открыть любой отчет, нажав на его название.

- Интерфейс приложения Kaspersky Security Center 13 Web Console и справка теперь доступны на корейском языке.

- Доступен новый подраздел Объявления "Лаборатории Касперского" в разделе **Мониторинг и отчеты**. В этом разделе предоставлена информация о вашей версии Kaspersky Security Center и управляемых приложениях, установленных на управляемых устройствах. Kaspersky Security Center периодически обновляет информацию в разделе, удаляет устаревшие объявления и добавляет новую информацию. Вы можете отключить объявления "Лаборатории Касперского".

- Реализована дополнительная аутентификация после изменения параметров учетной записи пользователя. Вы можете включить защиту учетной записи пользователя от несанкционированного изменения. Если этот параметр включен, изменение параметров учетной записи пользователя требует авторизации пользователя с правами на изменение.

В приложении Kaspersky Security Center 13 были реализованы следующие функции:

- Внедрена двухфакторная аутентификация. Вы можете включить двухфакторную аутентификацию для снижения риска несанкционированного доступа к Консоли администрирования. Если этот параметр включен, изменение параметров учетной записи пользователя требует авторизации пользователя с правами на изменение. Теперь вы можете включить или выключить двухфакторную аутентификацию для KES-устройств.

- Вы можете отправлять сообщения на Сервер администрирования через HTTP. Доступны справочное руководство и библиотека Python для работы с OpenAPI Сервера администрирования.

- Вы можете выпустить резервный сертификат для использования в iOS MDM-профилях, чтобы обеспечить переключение управляемых iOS-устройств после истечения срока действия сертификата Сервера iOS MDM.

- Папка мультитенантных приложений больше не отображается в Консоли администрирования.

Исправленные ошибки

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

Список проблем, исправленных в Kaspersky Security Center 15.1 Update 3

Версия Kaspersky Security Center, в которой проблема появилась впервые	Идентификатор проблемы	Описание проблемы
15.1	8646684	Некорректно работал фильтр отображения устройств при указании IP-адреса с условием "Не равно".
15.1	9548661	При добавлении категории приложений могла некорректно рассчитываться хеш-сумма по алгоритму SHA256, из-за чего мог не работать компонент Контроль приложений.
15.1	9624350	Задача обновления Kaspersky Endpoint Security оставалась в состоянии **Ожидает выполнения**, хотя на управляемом устройстве она уже была успешно завершена.
15.1	9649658	Для приложений, не поддерживаемых функцией **Системное администрирование**, задача *Поиск уязвимостей и требуемых обновлений* завершалась с предупреждением об ошибках выполнения.
15.1	9793319	Задача *Установка требуемых обновлений и закрытие уязвимостей* могла завершаться с ошибкой "System error 0xC1 (%1 не является приложением Win32.)".
15.1	10007988	Установка Агента администрирования на устройствах под управлением Microsoft Windows ARM могла зависать на этапе **Проверка подключения к Серверу администрирования**.
15.1	10018345	При сканировании контроллера домена могла возникать ошибка, связанная с некорректной обработкой строк.
15.1	9991501	В автоматически обновляемой категории приложений не обновлялся список хешей файлов, если длина пути к одному или нескольким файлам в исходной папке превышала 260 символов.
15.1	9973938	При высокой нагрузке процесс `ksnproxy` завершался с ошибкой.
15.1	9973938	В отчетах некорректно отображались корейские символы.
15.1	10064419	Отчет о состоянии правил Адаптивного контроля аномалий мог отображаться пустым.
15.1	10111675	При интеграции с SIEM события могли записываться в базу данных с задержкой от 5 до 15 минут вместо записи в режиме реального времени.
15.1	10100066	Web Console могла завершать сессию пользователя с ошибкой при большом количестве групп администрирования.
15.1	9829027	Отчет об используемых антивирусных базах мог не создаваться при использовании фильтра **Статус антивирусных баз**.
15.1	10308973	Задача *Поиск уязвимостей и обновлений сторонних производителей, перечисленных "Лабораторией Касперского"* могла сообщать о необходимости обновить AnyDesk, даже если на устройстве уже была установлена последняя версия приложения.
15.1	10373593	Задача загрузки обновлений в хранилище могла оставаться в статусе **Ожидает выполнения** после успешного завершения.
15.1	10466140	При создании категории приложений в поле **Хеш файла** можно было ввести кириллические символы, которые не соответствуют формату хеша.
15.1	10432122	Создание категорий приложений, содержащих более 100 000 записей, могло приводить к повреждению хранилища данных Kaspersky Security Center.
15.1	10295283	Задача *Поиск уязвимостей и требуемых обновлений* завершалась с ошибкой из-за сбоя синхронизации с WSUS.

15.1	10514034	После опроса контроллеров домена в Консоли администрирования могла отображаться неполная структура организационных подразделений.
15.1	10588197	При создании инсталляционного пакета Агента администрирования для macOS Сервер администрирования мог завершать работу с ошибкой.
15.1	8616680	В Web Console для некоторых параметров вместо локализованного текста отображались ключи локализации.
15.1	10734867	При запуске Агент администрирования мог сообщать об ошибке запуска службы Windows Update, если служба была отключена и в политике Агента администрирования был отключен параметр **Информация об обновлениях Центра обновления Windows**.
14.2	8801755	На устройствах под управлением Microsoft Windows Server 2019 Datacenter задача *Установка требуемых обновлений и закрытие уязвимостей* зависала со статусом **В ожидании завершения работы**, если в параметрах задачи была включена установка обновлений Windows при перезагрузке или выключении системы. На устройствах под управлением Microsoft Windows Server 2022 Datacenter ошибка сохраняется.
14.2	8996834	После успешной установки Агента администрирования задача установки не завершалась.
14.2	9132082	Агент администрирования версии 10.5 не мог подключиться к Серверу администрирования версии 14.2 через шлюз соединения с Агентом администрирования версии 14.0.
14.2	9243975	При большом объеме служебных данных Сервер администрирования завершал работу с ошибкой о нехватке оперативной памяти.
11.0	3331539	После обновления Kaspersky Endpoint Security до версии 11 с более ранних версий могло отображаться сообщение **Для Kaspersky Security Center требуется установка плагинов**. При переходе по ссылке из сообщения открывалось пустое окно.

О Kaspersky Security Center

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

Информация в справке может отличаться от информации в документах, входящих в состав комплекта документов к приложению. В этом случае актуальной считается информация в справке. Перейти в справку можно по ссылкам, встроенным в интерфейс приложения, или по ссылке из документации. Справка может обновляться без уведомления. При необходимости вы можете переключаться между онлайн-справкой и офлайн-справкой.

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

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

При помощи Kaspersky Security Center вы можете:

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

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

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

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

- Централизованно создавать образы операционных систем и разворачивать их на клиентских устройствах по сети, а также выполнять удаленную установку приложений "Лаборатории Касперского" и других производителей программного обеспечения.

- Удаленно управлять приложениями "Лаборатории Касперского" и других производителей, установленными на клиентских устройствах: Устанавливать обновления, искать и закрывать уязвимости.

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

- Получать статистику и отчеты о работе приложений и устройств.

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

- Управлять мобильными устройствами.

- Управлять шифрованием информации, хранящейся на жестких дисках устройств и съемных дисках, и доступом пользователей к зашифрованным данным.

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

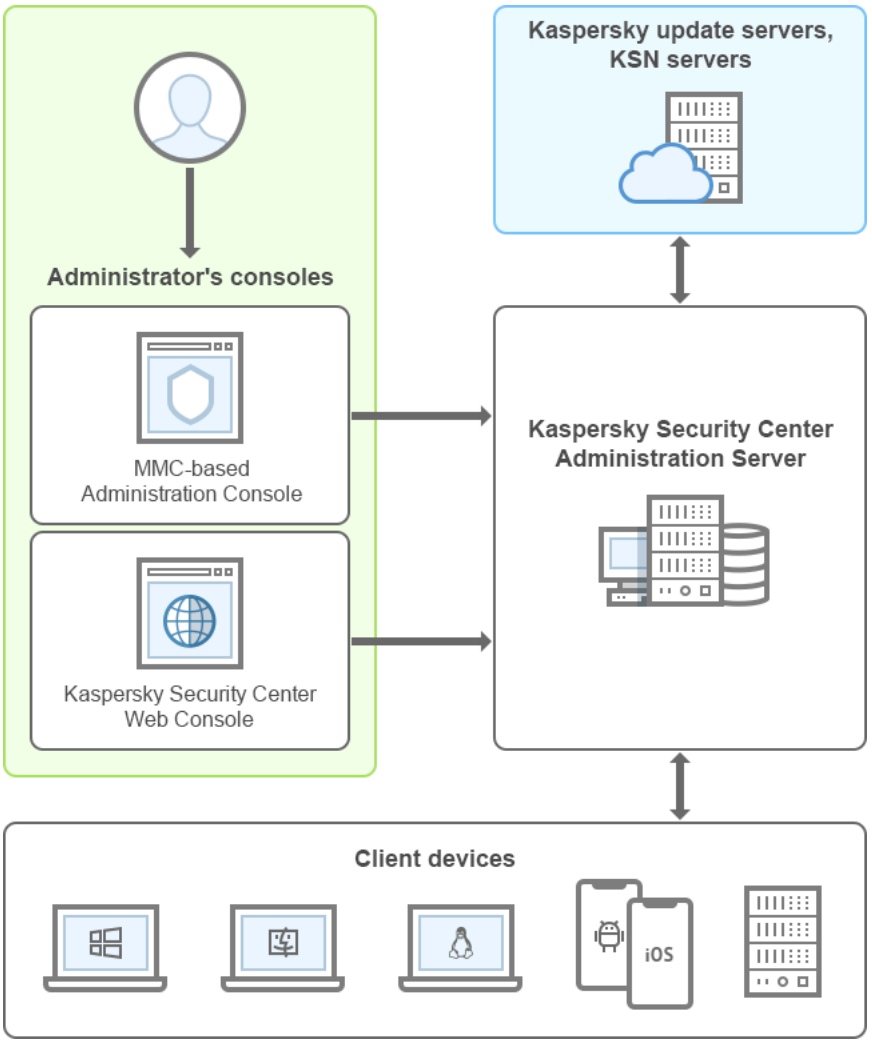
Вы можете приобрести Kaspersky Security Center через "Лабораторию Касперского" (например, на сайте https://www.kaspersky.ru) или через компании-партнеров.

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

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

Архитектура

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



Архитектура приложения Kaspersky Security Center

Приложение Kaspersky Security Center включает в себя следующие основные компоненты:

- *Консоль администрирования* (далее также *Консоль*). Предоставляет пользовательский интерфейс к административным службам Сервера и Агента. Консоль администрирования выполнена в виде компонента расширения к Microsoft Management Console (MMC). Консоль администрирования позволяет подключаться к удаленному Серверу администрирования через интернет.

- *Kaspersky Security Center Web Console*. Представляет собой веб-интерфейс для создания и управления системой защиты сети организации-клиента, находящейся под управлением Kaspersky Security Center.

- *Сервер администрирования Kaspersky Security Center* (далее также *Сервер*). Осуществляет функции централизованного хранения информации об установленных в сети организации приложениях и управления ими.

- *Серверы обновлений "Лаборатории Касперского"*. HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложений.

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

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

Аппаратные и программные требования

- Требования Сервера администрирования
- Требования Web Console
- Требования серверов мобильных устройств
- Требования Консоли администрирования
- Требования Агента администрирования

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

Требования Сервера администрирования

Минимальные аппаратные требования:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 4 ГБ.
- Объем свободного места на диске: 10 ГБ. При использовании функциональности Системное администрирование объем свободного места на диске должен быть не менее 100 ГБ.

Для развертывания в облачных окружениях требования к Серверу администрирования и серверу базы данных такие же, как и к физическому Серверу администрирования (в зависимости от того, каким количеством устройств вы хотите управлять).

Программные требования:

- Microsoft Data Access Components (MDAC) 2.8.
- Microsoft Windows DAC 6.0.
- Microsoft Windows Installer 4.5.

Поддерживаются следующие операционные системы:

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

- Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64-разрядная.
- Windows Server 2016 Standard/Datacenter/Essentials/Server Core (варианты установки) (LTSB) 64-разрядная.
- Windows Server 2019 Standard/Datacenter/Core 64-разрядная.
- Windows Server 2022 Standard/Datacenter/Core 64-разрядная.
- Windows Server 2025 Standard/Datacenter/Core 64-разрядная.
- Windows Storage Server 2019 64-разрядная.

Поддерживаются следующие платформы виртуализации:

- VMware vSphere 6.7.
- VMware vSphere 7.0.
- VMware vSphere 8.0.
- Microsoft Hyper-V Server 2019 64-разрядная.
- Microsoft Hyper-V Server 2022 64-разрядная.
- Citrix XenServer 7.1 LTSR.

- Citrix XenServer 8.x.
- Parallels Desktop 18.
- Oracle VM VirtualBox 7.x.

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

- Microsoft SQL Server 2017 (все редакции) для Windows/Linux 64-разрядная.
- Microsoft SQL Server 2019 (все редакции) для Windows/Linux 64-разрядная (требуются дополнительные действия).
- Microsoft SQL Server 2022 (все редакции) для Windows/Linux 64-разрядная.
- Microsoft SQL Server 2025 (все редакции) для Windows/Linux 64-разрядная.
- MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная.
- MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная.
- MariaDB 10.5 (сборка 10.5.27 и выше) 32-разрядная/64-разрядная.
- MariaDB 11.4 LTS 64-разрядная.
- MariaDB 11.8 LTS 64-разрядная.
- MariaDB 12.3 LTS 64-разрядная.
- MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
- PostgreSQL 15.x 64-разрядная.
- Postgres Pro 16.x (все редакции) 64-разрядная.
- Postgres Pro 17.x (все редакции) 64-разрядная.
- Postgres Pro 18.x (все редакции) 64-разрядная.

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

Сведения и ограничения см. в разделе: Выбор СУБД.

SIEM-системы и другие системы управления информацией:

- HP (Micro Focus) ArcSight ESM 7.0.
- IBM QRadar 7.3.
- Splunk 7.1.

Требования Web Console

Сервер Kaspersky Security Center Web Console

Минимальные аппаратные требования:

- Процессор: 4 ядра, частота от 2500 МГц.
- Оперативная память: 8 ГБ.
- Объем свободного места на диске: 40 ГБ.

Минимальные требования к сертификату Сервера администрирования:

- Алгоритм подписи сертификата SHA-2.
- Минимальная длина ключа 2048.

Если вам нужно перевыпустить сертификат, см. Базу знаний Kaspersky Security Center.

Операционные системы, поддерживаемые Сервером Kaspersky Security Center Web Console

Операционные системы. Microsoft Windows (только 64-разрядные версии) Для межпроцессного взаимодействия в операционной системе необходим доступ к интерфейсу обратной связи (loopback).	Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials/Server Core. Windows Server 2016 Standard/Datacenter/Essentials/Server Core (варианты установки) (LTSB). Windows Server 2019 Standard/Datacenter/Core. Windows Server 2022 Standard/Datacenter/Core. Windows Server 2025 Standard/Datacenter/Core. Windows Storage Server 2019.
Платформы виртуализации	VMware vSphere 6.7. VMware vSphere 7.0. VMware vSphere 8.0. Citrix XenServer 7.1 LTSR. Citrix XenServer 8.x. Parallels Desktop 18. Oracle VM VirtualBox 7.x.

Клиентские устройства

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

Минимальное разрешение экрана составляет 1366x768 пикселей.

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

Браузеры:

- Google Chrome 128.0.6613.120.
- Microsoft Edge 128.0.2739.67.
- Safari 17.6 для macOS.
- Яндекс Браузер 24.7.3.1081.
- Mozilla Firefox Extended Support Release 115.14.0.

Требования серверов мобильных устройств

Сервер мобильных устройств iOS Mobile Device Management (iOS MDM)

Аппаратные требования:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 2 ГБ.
- Объем свободного места на диске: 2 ГБ.

Операционная система Microsoft Windows (версия поддерживаемой операционной системы определяется требованиями Сервера администрирования).

Требования Консоли администрирования

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.

Программные требования:

- Операционная система Microsoft Windows (версия поддерживаемой операционной системы определяется требованиями Сервера администрирования):
  - Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials 64-разрядная.
  - Windows Server 2016 Standard/Datacenter/Essentials (LTSB) 64-разрядная.
  - Windows Server 2019 Standard/Datacenter 64-разрядная.

    - Windows Server 2022 Standard/Datacenter 64-разрядная.
    - Windows Server 2025 Standard/Datacenter/Core 64-разрядная.
    - Windows Storage Server 2019 64-разрядная.
- Microsoft Management Console 2.0.
- Microsoft Windows Installer 4.5.
- Microsoft Internet Explorer 11.0 работает на:
    - Microsoft Windows Server 2012 R2.
    - Microsoft Windows Server 2016.
    - Microsoft Windows Server 2019.
    - Microsoft Windows Storage Server 2019.
- Microsoft Edge, запущенный на Microsoft Windows Server 2022 Standard.

Требования Агента администрирования

Минимальные аппаратные требования:

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

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

Операционные системы. Microsoft Windows	Windows Embedded POSReady 2009 с последним Service Pack 32-разрядная. Windows Embedded 7 Standard Service Pack 1 32-разрядная/64-разрядная. Windows Embedded 8.1 Industry Pro 32-разрядная/64-разрядная. Windows 10 Enterprise 2015 LTSB 32-разрядная/64-разрядная. Windows 10 Enterprise 2016 LTSB 32-разрядная/64-разрядная. Windows 10 IoT Enterprise 2015 LTSB 32-разрядная/64-разрядная. Windows 10 IoT Enterprise 2016 LTSB 32-разрядная/64-разрядная. Windows 10 Enterprise 2019 LTSC 32-разрядная/64-разрядная. Windows 10 IoT Enterprise версия 1703 32-разрядная/64-разрядная. Windows 10 IoT Enterprise версия 1709 32-разрядная/64-разрядная. Windows 10 IoT Enterprise версия 1803 32-разрядная/64-разрядная. Windows 10 IoT Enterprise версия 1809 32-разрядная/64-разрядная. Windows 10 20H2 IoT Enterprise 32-разрядная/64-разрядная. Windows 10 21H2 IoT Enterprise 32-разрядная/64-разрядная. Windows 10 IoT Enterprise 32-разрядная/64-разрядная. Windows 10 IoT Enterprise версия 1909 32-разрядная/64-разрядная. Windows 10 IoT Enterprise LTSC 2021 32-разрядная/64-разрядная. Windows 10 IoT Enterprise версия 1607 32-разрядная/64-разрядная. Windows 10 TH1 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Windows 10 TH2 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Windows 10 RS1 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Windows 10 RS2 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Windows 10 RS3 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Windows 10 RS4 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Windows 10 RS5 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Windows 10 RS6 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Windows 10 19H1 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Windows 10 19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Windows 10 20H1 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Windows 10 20H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Windows 10 21H1 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Windows 10 21H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Windows 10 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-разрядная/64-разрядная. Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM 64-разрядная. Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная. Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная. Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная. Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-разрядная. Windows 8 Pro/Enterprise 32-разрядная/64-разрядная. Windows 8.1 Pro/Enterprise 32-разрядная/64-разрядная. Windows 7 Home/Pro/Enterprise/Ultimate Service Pack 1 32-разрядная/64-разрядная. Microsoft Windows XP Professional Service Pack 2 32-разрядная/64-разрядная (поддерживаются только для Агента администрирования обновленной версии 10.5.1781, которую вы можете запросить в Службе технической поддержки). Windows XP Professional Service Pack 3 и выше 32-разрядная (поддерживается Агентом администрирования версии 14.0.0.20145). Windows XP Professional for Embedded Systems Service Pack 3 32-разрядная (поддерживается Агентом администрирования версии 14.0.0.20145). Windows MultiPoint Server 2011 Standard/Premium 64-разрядная. Windows Server 2003 SP1 32-разрядная/64-разрядная (поддерживается Агентом администрирования обновленной версии 10.5.1781). Windows Server 2003 SP2 Standard/Enterprise 32-разрядная/64-разрядная (поддерживается Агентом администрирования обновленной версии 10.5.1781). Windows Server 2003 R2 Standard/Enterprise SP2 32-разрядная/64-разрядная (поддерживается Агентом администрирования обновленной версии 10.5.1781). Windows Server 2008 R2 Standard/Datacenter/Enterprise/Foundation/ Service Pack 1 и выше 64-разрядная. Windows Server 2012 Standard/Datacenter/Essentials/Foundation/Server Core 64-разрядная.

	Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64-разрядная. Windows Server 2016 Standard/Datacenter/Essentials/Server Core (варианты установки) (LTSB) 64-разрядная. Windows Server 2019 Standard/Datacenter/Core 64-разрядная. Windows Server 2019 RS5 Standard/Essentials 64-разрядная. Windows Server 2022 Standard/Datacenter/Core 64-разрядная. Windows Server 2022 21H2 Standard/Datacenter 64-разрядная. Windows Server 2025 Standard/Datacenter/Core 64-разрядная. Windows Storage Server 2019 64-разрядная.

Операционные системы. Linux	Debian GNU/Linux 10.x (Buster) 32-разрядная/64-разрядная. Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная. Debian GNU/Linux 12 (Bookworm) 32-разрядная/64-разрядная. Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная. Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная. Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная. Ubuntu Server 22.04 LTS ARM 64-разрядная. Ubuntu Server 24.04 LTS (Noble Numbat) 64-разрядная. CentOS 6.7 и выше 32-разрядная. CentOS 6.x (до 6.6) 32-разрядная/64-разрядная. CentOS 7.x 64-разрядная. CentOS Stream 8 64-разрядная. CentOS Stream 9 64-разрядная. CentOS Stream 9 ARM 64-разрядная. Red Hat Enterprise Linux Server 6.x 32-разрядная/64-разрядная. Red Hat Enterprise Linux Server 7.x 64-разрядная. Red Hat Enterprise Linux Server 8.x 64-разрядная. Red Hat Enterprise Linux Server 9.x 64-разрядная. SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная. SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная. SUSE Linux Enterprise Server 15 (все пакеты обновлений) ARM 64-разрядная. openSUSE 15 64-разрядная. EulerOS 2.0 SP10 64-разрядная. EulerOS 2.0 SP10 ARM 64-разрядная. Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5) 64-разрядная. Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6) 64-разрядная. Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6) 64-разрядная. Astra Linux Special Edition РУСБ.10015-17 (очередное обновление 1.7.3) 64-разрядная. Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7) 64-разрядная. Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8) 64-разрядная. Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7) 64-разрядная. Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7) ARM 64-разрядная. Astra Linux Common Edition (очередное обновление 2.12) 64-разрядная. Альт Рабочая станция 10.1 64-разрядная. Альт Сервер 10.1 64-разрядная. Альт Образование 10.1 64-разрядная. Альт СП Сервер 10 32-разрядная/64-разрядная. Альт СП Сервер 10 ARM 64-разрядная. Альт СП Рабочая станция 10 32-разрядная/64-разрядная. Альт СП Рабочая станция 10 ARM 64-разрядная. Альт Сервер 10 64-разрядная. Альт Сервер 10 ARM 64-разрядная. Альт Рабочая станция 10 32-разрядная/64-разрядная. Альт 8 СП Рабочая станция (8.4) ARM 64-разрядная. Альт 8 СП Сервер (8.4) ARM 64-разрядная. Альт 8 СП Сервер (ЛКНВ.11100-01) 32-разрядная/64-разрядная. Альт 8 СП Сервер (ЛКНВ.11100-02) 32-разрядная/64-разрядная. Альт 8 СП Сервер (ЛКНВ.11100-03) 32-разрядная/64-разрядная. Альт 8 СП Рабочая станция (ЛКНВ.11100-01) 32-разрядная/64-разрядная. Альт 8 СП Рабочая станция (ЛКНВ.11100-02) 32-разрядная/64-разрядная. Альт 8 СП Рабочая станция (ЛКНВ.11100-03) 32-разрядная/64-разрядная. Mageia 4 32-разрядная. Oracle Linux 7 64-разрядная. Oracle Linux 8 64-разрядная. Oracle Linux 9 64-разрядная. Linux Mint 20.x 64-разрядная.

	Linux Mint 21.1 и выше 64-разрядная. AlterOS 7.5 или выше 64-разрядная. ГосЛинукс IC6/7.17 64-разрядная. ГосЛинукс IC6/7.2 64-разрядная. SberOS 3.3.1 64-разрядная. Platform V SberLinux OS Server (SLO) 8.8 64-разрядная. Platform V SberLinux OS Server (SLO) 8.9.2 64-разрядная. РЕД ОС 7.3 ARM 64-разрядная. РЕД ОС 7.3 Сервер 64-разрядная. РЕД ОС 7.3 Сертифицированная редакция 64-разрядная. РЕД ОС 8 Сертифицированная редакция 64-разрядная. ROSA Enterprise Linux Server 7.9 64-разрядная. ROSA Enterprise Linux Desktop 7.9 64-разрядная. РОСА "КОБАЛЬТ" 7.9 64-разрядная. РОСА "ХРОМ" 12 64-разрядная. AlmaLinux 8 и выше 64-разрядная. AlmaLinux 9 и выше 64-разрядная. Rocky Linux 8 и выше 64-разрядная. Rocky Linux 9 и выше 64-разрядная. Атлант, сборка Alcyone, версия 2022.02 64-разрядная. МСВСфера 9.2 Сервер 64-разрядная. МСВСфера 9.2 АРМ 64-разрядная. СинтезМ Сервер 8.6 64-разрядная. СинтезМ Клиент 8.6 64-разрядная. ОСнова 2.10 64-разрядная. Kylin 10 64-разрядная. EMIAS 1.0 64-разрядная. Amazon Linux 2 64-разрядная. МосОС 15.4 Arbat 64-разрядная. ОС МЭШ (Moscow Electronic School) 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.

Поддерживаются следующие платформы виртуализации:

- VMware vSphere 6.7.
- VMware vSphere 7.0.
- VMware vSphere 8.0.
- Parallels Desktop 18.
- Oracle VM VirtualBox 7.x.
- Citrix XenServer 7.1 LTSR.
- Citrix XenServer 8.x.
- KVM (Kernel-based Virtual Machine).

В версиях Windows ниже версий Microsoft Windows Server 2008 R2 (серверные версии) и Microsoft Windows 7 (декстопные версии), Агент администрирования не поддерживает следующие функции:

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

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

Перед установкой Агента администрирования на устройства под управлением Windows 7 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 R2 x64 Edition (KB3063858).

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

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

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

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

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

Совместимые приложения и решения "Лаборатории Касперского"

Kaspersky Security Center поддерживает централизованное развертывание и управление всеми поддерживаемыми на данный момент приложениями и решениями "Лаборатории Касперского". В таблице ниже показано, какие приложения и решения "Лаборатории Касперского" поддерживаются Консолью администрирования на основе MMC и Kaspersky Security Center Web Console. Подробнее о версиях приложений и решений см. на странице "Жизненный цикл приложений".

Название приложения "Лаборатории Касперского" или решения	Поддерживается Консоль администрирования на основе MMC	Поддерживается Kaspersky Security Center Web Console
Для рабочих станций		
Kaspersky Endpoint Security для Windows	✓	✓
Kaspersky Endpoint Security для Linux	✓	✓
Kaspersky Endpoint Security для Linux Elbrus Edition	✓	✓
Kaspersky Endpoint Security для Mac	✓	✓
Kaspersky Endpoint Agent	✓	✓
Kaspersky Embedded Systems Security для Windows	✓	✓
Kaspersky Embedded Systems Security для Linux	—	✓
Kaspersky Password Manager для бизнеса	—	✓
Для промышленных решений		
Kaspersky Industrial CyberSecurity for Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Linux Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Networks (централизованное развертывание не поддерживается)	✓	✓
Для мобильных устройств		
Kaspersky Endpoint Security для Android	✓	✓
Kaspersky Security для iOS	—	✓
Для файловых серверов:		
Kaspersky Security для Windows Server	✓	✓
Kaspersky Endpoint Security для Windows	✓	✓
Kaspersky Endpoint Security для Linux	✓	✓
Для виртуальных сред		
Kaspersky Security для виртуальных сред Легкий агент	✓	✓
Kaspersky Security для виртуальных сред Защита без агента	✓	—
Для обнаружения целевых атак		
Kaspersky Sandbox Server	—	✓
Kaspersky Endpoint Detection and Response Optimum	—	✓
Kaspersky Managed Detection and Response	—	✓
Для устройств с операционной системой KasperskyOS		
Kaspersky IoT Secure Gateway	—	✓
Kaspersky Thin Client	—	✓
Репутационные базы данных		
Kaspersky Private Security Network	—	✓

Лицензии и возможности Kaspersky Security Center 15.1

Kaspersky Security Center требует лицензии на некоторые его функции.

В таблице ниже показано, какая лицензия охватывает какие функции Kaspersky Security Center.

Чтобы использовать функции Kaspersky Security Center, необходимо активировать Сервер администрирования, добавив лицензионный ключ Сервера администрирования.

Необходимо вручную добавить лицензионный ключ для каждого Сервера администрирования.

Лицензии и возможности Kaspersky Security Center

Функции Kaspersky Security Center	Системное администрирование	Kaspersky Endpoint Security для бизнеса Стандартный	Kaspersky Endpoint Security для бизнеса Расширенный	Kaspersky Total Security для бизнеса	Kaspersky Security для виртуальных и облачных сред Standard	Kaspersky Security для виртуальных и облачных сред Enterprise	Kaspers EDR Optimum
Поиск уязвимости	✓	✓	✓	✓	✓	✓	✓
Управление патчами	✓	–	✓	✓	–	✓	✓
Управление доступом на основе ролей	✓	✓	✓	✓	✓	✓	✓
Установка операционных систем и приложений	✓	–	✓	✓	–	✓	✓
Управление мобильными устройствами (то есть управление iOS- и Android-устройствами пользователей)	✓	✓	✓	✓	–	–	✓
Настройка облачного окружения для работы в облачных окружениях, таких как AWS, Microsoft Azure или Google Cloud	–	–	–	–	✓	✓	–
Экспорт событий в SIEM-системы: Syslog	✓	✓	✓	✓	✓	✓	✓
Экспорт событий в SIEM-системы: QRadar by IBM и ArcSight от Micro Focus	✓	✓	✓	✓	✓	✓	✓

О совместимости компонентов Kaspersky Security Center

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

Совместимость компонентов Kaspersky Security Center

Компонент	Совместим с
Сервер администрирования Kaspersky Security Center 15.1	• Консоль администрирования Kaspersky Security Center 15.1. • Kaspersky Security Center 15.1 Web Console. • Агент администрирования Kaspersky Security Center версий: 17, 14*, 10.5**.
Kaspersky Security Center 15.1 Web Console	Сервер администрирования Kaspersky Security Center следующих версий: 15.1.
Главный Сервер администрирования Kaspersky Security Center 15.1	Подчиненные Серверы администрирования: • Kaspersky Security Center Windows следующих версий: 15.1. • Kaspersky Security Center Linux следующих версий: 14.2, 15, 15.1, 15.2, 15.3, 15.4, 16, 16.1, 16.2, 16.3.
Подчиненный Сервер администрирования Kaspersky Security Center 15.1	Главные Серверы администрирования: • Kaspersky Security Center Windows следующих версий: 15.1. • Kaspersky Security Center Linux следующих версий: 14.2, 15, 15.1, 15.2, 15.3, 15.4, 16, 16.1, 16.2, 16.3.

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

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

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

Если у вас есть последняя версия Kaspersky Security Center Web Console и предыдущая версия Kaspersky Security Center и во время настройки параметров подключения к домену происходит ошибка, текст ошибки содержит стандартное сообщение.

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

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

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

Функция или свойство	Kaspersky Security Center	
	Решение на базе Windows	Решение на базе Linux
Сервер администрирования		
Расположение системы управления базами данных (СУБД)	В локальной инфраструктуре	В локальной инфраструктуре (Microsoft SQL не поддерживается)
Операционная система для установки Сервера администрирования	Windows	Linux
Иерархия Серверов администрирования	✓	✓
Поддержка виртуальных Серверов администрирования	✓	✓
Использование SNMP для отправки статистики Сервера администрирования приложениям сторонних производителей	✓	Будет реализовано в 2026 году
Веб-сервер для публикации инсталляционных пакетов и других файлов	✓	✓
Установка Сервера администрирования на односайтовом отказоустойчивом кластере Windows Server	✓	—
Развертывание отказоустойчивого кластера Kaspersky Security Center	✓ Только односайтовый отказоустойчивый кластер	✓ Начиная с версии Kaspersky Security Center 16.2 Linux поддерживается геораспределенный отказоустойчивый кластер.
Консоль администрирования		
Тип Консоли администрирования	На базе MMC и веб-интерфейс	Веб-интерфейс
Операционная система для установки Консоли администрирования с веб-интерфейсом	Windows или Linux	Linux
Вход в консоль с использованием доменной аутентификации	✓	✓ Технология единого входа не поддерживается для версий 15.1–15.4 включительно
Управление клиентскими устройствами и группами администрирования		
Максимальное количество управляемых устройств (на один Сервер администрирования)	100 000	50 000 (с PostgreSQL и Postgres Pro)
Опрос сети	✓	✓ Начиная с версии 16, поддерживаются контроллеры домена FreeIPA и ALD Pro.
Защита устройств под управлением Windows, macOS и Linux	✓	✓
Защита мобильных устройств	✓ Базовое управление мобильными устройствами	✓ MDM и использование функциональности Kaspersky Secure Mobility Management (по лицензии).
Управление защитой виртуальных машин	✓	✓
Защита публичной облачной инфраструктуры	✓	—
Удаленное подключение к рабочему столу клиентского устройства	✓	✓ Начиная с версии 15.3.
Шифрование и защита данных	✓	✓ На управляемых устройствах с операционной системой Windows с установленным Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Mac.

Функция или свойство	Kaspersky Security Center	
	Решение на базе Windows	Решение на базе Linux
Поддержка кластеров и массивов серверов в группах администрирования	✓	✓
Иерархия групп администрирования	✓	✓
Добавление шлюза соединения в демилитаризованной зоне в качестве точки распространения	✓ (Консоль администрирования на основе MMC)	Будет реализовано в 2026 году
Работа с пользователями		
Создание учетных записей пользователей, контроль учетных записей	✓	✓
Управление приложениями "Лаборатории Касперского"		
Политики приложений	✓	✓
Задачи для приложений "Лаборатории Касперского"	✓	✓
Kaspersky Security Network	✓	✓
Прокси-сервер KSN	✓	✓
Kaspersky Private Security Network	✓	✓
Централизованное распространение лицензионных ключей приложений "Лаборатории Касперского"	✓	✓
Удаленная диагностика клиентских устройств	✓	✓
Автоматическое обновление приложений "Лаборатории Касперского"	✓	✓
Поддержка Адаптивного контроля аномалий	✓	✓
Управление безопасностью устройств	✓	✓
Управление безопасностью, ориентированной на пользователя	✓	✓
Управление системами		
Развертывание операционных систем на клиентских устройствах	✓	—
Управление сторонними лицензиями	✓	—
Использовать Сервер администрирования в роли WSUS-сервера	✓	✓ (только в пассивном режиме поиска Центра обновления Windows)
Управление приложениями сторонних производителей на клиентских устройствах		
Установка обновлений приложений сторонних производителей и поиск уязвимостей в приложениях сторонних производителей	✓	✓
Мониторинг, отчеты и аудит		
Работа с ревизиями объектов	✓	✓
Сравнение ревизий политики	✓	Будет реализовано в 2026 году
Просмотр и работа с алертами, обнаруженными Kaspersky Endpoint Detection and Response Optimum	✓	✓
Уведомления о событиях, произошедших на управляемых устройствах	✓	✓

Функция или свойство	Kaspersky Security Center	
	Решение на базе Windows	Решение на базе Linux
Мониторинг состояния политик и задач	✓	✓
Интеграции		
Интеграция с Kaspersky Managed Detection and Response	✓	✓
Интеграция с SIEM-системами	✓	✓
Экспорт событий в форматах CEF и LEEF	✓	✓
Агрегирование алертов и выполнение действий по реагированию с помощью Active Directory, KASAP и Kaspersky TIP Sandbox	–	✓ (начиная с версии 15.4) Вам нужно активировать Сервер администрирования по лицензии Kaspersky Security для бизнеса Профессиональный, а затем распространить лицензионный ключ Kaspersky Security для бизнеса Профессиональный на управляемые приложения

О Kaspersky Security Center Cloud Console

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

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

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

- английском;
- французском;
- немецком;
- итальянском;
- японском;
- португальском (Бразилия);
- русском;
- упрощенном китайском;
- испанском;

- испанском (Латинская Америка);
- традиционном китайском.

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

Kaspersky Security Center 15.1

В этом разделе представлена информация об использовании Kaspersky Security Center 15.1.

Информация в справке может отличаться от информации в документах, входящих в состав комплекта документов к приложению. В этом случае актуальной считается информация в справке. Перейти в справку можно по ссылкам, встроенным в интерфейс приложения, или по ссылке из документации. Справка может обновляться без уведомления. При необходимости вы можете переключаться между онлайн-справкой и офлайн-справкой.

Основные понятия

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

Сервер администрирования

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

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

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

- под именем "Kaspersky Security Center Administration Server";
- с автоматическим типом запуска при старте операционной системы;
- с учетной записью **LocalSystem** либо учетной записью пользователя в соответствии с выбором, сделанным при установке Сервера администрирования.

Сервер администрирования выполняет следующие функции:

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

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

Правило именования Серверов администрирования в интерфейсе приложения

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

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

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

Иерархия Серверов администрирования

Серверы администрирования могут образовывать иерархию. Каждый Сервер администрирования может иметь несколько подчиненных Серверов администрирования (далее также *подчиненных Серверов*) на разных уровнях иерархии. Уровень вложенности подчиненных Серверов не ограничен. При этом в состав групп администрирования главного Сервера будут входить клиентские устройства всех подчиненных Серверов. Таким образом, независимые участки компьютерной сети могут управляться различными Серверами администрирования, которые, в свою очередь, управляются главным Сервером.

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

Иерархию Серверов администрирования можно использовать для следующих целей:

- Ограничение нагрузки на Сервер администрирования (по сравнению с одним установленным в сети Сервером).
- Сокращение трафика внутри сети и упрощение работы с удаленными офисами. Нет необходимости устанавливать соединение между главным Сервером и всеми устройствами сети, которые могут находиться, например, в других регионах. Достаточно установить на каждом участке сети подчиненный Сервер администрирования, распределить устройства в группах администрирования подчиненных Серверов и обеспечить подчиненным Серверам соединение с главным Сервером по быстрым каналам связи.
- Разделение ответственности между администраторами антивирусной безопасности. При этом сохраняются все возможности централизованного управления и мониторинга состояния антивирусной безопасности сети организации.
- Использование Kaspersky Security Center поставщиками услуг. Поставщику услуг достаточно установить Kaspersky Security Center и Kaspersky Security Center Web Console. Для управления большим числом клиентских устройств различных организаций поставщик услуг может включать в иерархию Серверов администрирования подчиненные Серверы администрирования (включая виртуальные Серверы).

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

Виртуальный Сервер администрирования

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

Виртуальный Сервер администрирования является частным случаем подчиненного Сервера администрирования и, по сравнению с физическим Сервером администрирования, имеет следующие основные ограничения:

- Виртуальный Сервер администрирования может функционировать только в составе главного Сервера администрирования.
- Виртуальный Сервер администрирования при работе использует основную базу данных главного Сервера администрирования. Задачи резервного копирования и восстановления данных, а также задачи проверки и загрузки обновлений, не поддерживаются на виртуальном Сервере администрирования.
- Для виртуального Сервера не поддерживается создание подчиненных Серверов администрирования (в том числе и виртуальных).

Кроме того, виртуальный Сервер администрирования имеет следующие ограничения:

- В окне свойств виртуального Сервера ограничен набор разделов.
- Для удаленной установки приложения "Лаборатории Касперского" на клиентские устройства, работающие под управлением виртуального Сервера, необходимо, чтобы на одном из клиентских устройств был установлен Агент администрирования для связи с виртуальным Сервером. При первом подключении к виртуальному Серверу администрирования это устройство автоматически назначается точкой распространения и выполняет роль шлюза соединений клиентских устройств с виртуальным Сервером администрирования.
- Виртуальный Сервер администрирования может опрашивать сеть только через точки распространения.
- Чтобы перезапустить виртуальный Сервер, работоспособность которого была нарушена, Kaspersky Security Center перезапускает главный Сервер администрирования и все виртуальные Серверы.
- Пользователям, которые были созданы на виртуальном Сервере, невозможно назначить роли на Сервере администрирования.

Администратор виртуального Сервера обладает всеми правами в рамках этого виртуального Сервера.

Сервер мобильных устройств

Сервер мобильных устройств – это компонент Kaspersky Security Center, который предоставляет доступ к мобильным устройствам и позволяет управлять ими через Консоль администрирования. Сервер мобильных устройств получает информацию о мобильных устройствах и хранит их профили.

Kaspersky Security Center включает Сервер iOS MDM в качестве Сервера мобильных устройств. Этот Сервер мобильных устройств используется для управления мобильными устройствами, поддерживающими сервис Apple Push Notifications (APNs).

Серверы мобильных устройств Kaspersky Security Center позволяют управлять следующими объектами:

- Отдельным мобильным устройством.
- Несколькими мобильными устройствами.
- Несколькими мобильными устройствами, подключенными к кластеру серверов, одновременно. При подключении к кластеру серверов Сервер мобильных устройств, установленный на этом кластере, отображается в Консоли администрирования как один сервер.

Веб-сервер

Веб-сервер Kaspersky Security Center (далее также *Веб-сервер*) – это компонент Kaspersky Security Center, который устанавливается в составе Сервера администрирования. Веб-сервер предназначен для передачи по сети автономных инсталляционных пакетов, iOS MDM-профилей, а также файлов из папки общего доступа.

При создании автономный инсталляционный пакет автоматически публикуется на Веб-сервере. Ссылка для загрузки автономного пакета отображается в списке созданных автономных инсталляционных пакетов. При необходимости вы можете отменить публикацию автономного пакета или повторно опубликовать его на Веб-сервере.

При создании iOS MDM-профиль для мобильного устройства пользователя также автоматически публикуется на Веб-сервере. Опубликованный профиль автоматически удаляется с Веб-сервера после успешной установки на мобильное устройство пользователя.

Папка общего доступа используется для размещения информации, доступной всем пользователям, устройства которых находятся под управлением Сервера администрирования. Если у пользователя нет прямого доступа к папке общего доступа, ему можно передать информацию из этой папки с помощью Веб-сервера.

Для передачи пользователям информации из папки общего доступа с помощью Веб-сервера администратору требуется создать в папке общего доступа вложенную папку public и поместить в нее информацию.

Синтаксис ссылки для передачи информации пользователю выглядит следующим образом:

```
https://<Web Server name>:<HTTPS port>/public/<object>
```

где:

- `<Web Server name>` – имя Веб-сервера Kaspersky Security Center.
- `<HTTPS port>` – HTTPS-порт Веб-сервера, заданный администратором. HTTPS-порт можно задать в разделе **Веб-сервер** окна свойств Сервера администрирования. По умолчанию установлен порт 8061.
- `<object>` – вложенная папка или файл, доступ к которым требуется открыть для пользователя.

Администратор может передать сформированную ссылку пользователю любым удобным способом, например, по электронной почте.

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

Агент администрирования

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

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. Вы можете активировать компонент следующими способами:

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

Нет необходимости устанавливать Агент администрирования на устройства, на которых установлен Сервер администрирования, поскольку серверная версия Агента администрирования устанавливается автоматически совместно с Сервером администрирования.

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

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

Группы администрирования

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

Для всех управляемых устройств в группе администрирования устанавливаются:

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

Управляемое устройство может входить в состав только одной группы администрирования.

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

Управляемое устройство

Управляемое устройство – это устройство под управлением Windows, Linux или macOS, на котором установлен Агент администрирования, или мобильное устройство, на котором установлено приложение безопасности "Лаборатории Касперского". Вы можете управлять такими устройствами с помощью задач и политик для приложений, установленных на устройствах. Вы также можете формировать отчеты для управляемых устройств.

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

Устройство может находиться под управлением только одного Сервера администрирования. Один Сервер администрирования может обслуживать до 100 000 устройств, включая мобильные устройства.

Нераспределенное устройство

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

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

Рабочее место администратора

Рабочее место администратора — устройство, на котором установлена Консоль администрирования или которое вы используете для работы с Kaspersky Security Center Web Console. С этих устройств администраторы могут осуществлять удаленное централизованное управление приложениями "Лаборатории Касперского", установленными на клиентских устройствах.

В результате установки Консоли администрирования на вашем устройстве появится значок для запуска Консоли администрирования. Найдите его в меню **Пуск → Приложения → Kaspersky Security Center**.

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

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

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

Плагин управления

Управление приложениями "Лаборатории Касперского" через Консоль администрирования выполняется при помощи специального компонента – *плагина управления*. В состав каждого приложения "Лаборатории Касперского", которым можно управлять при помощи Kaspersky Security Center, входит плагин управления.

С помощью плагина управления приложением в Консоли администрирования можно выполнять следующие действия:

- создавать и редактировать политики и параметры приложения, а также параметры задач этой приложения;
- получать информацию о задачах приложения, событиях в ее работе, а также о статистике работы приложения, получаемой с клиентских устройств.

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

Веб-плагин управления

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

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

Плагин управления предоставляет следующие возможности:

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

Политики

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

Tasks

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

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

Задачи могут выполняться на Сервере администрирования и на устройствах.

Задачи, которые выполняются на Сервере администрирования:

- автоматическая рассылка отчетов;
- загрузка обновлений в хранилище Сервера администрирования;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных;
- синхронизация обновлений Windows Update;
- создание инсталляционного пакета на основе образа операционной системы эталонного устройства.

На устройствах выполняются следующие типы задач:

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

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

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

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

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

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

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

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

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

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

Область действия задачи

Область 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.

Взаимосвязь политики и локальных параметров приложения

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

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

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

- Если на изменение параметра наложен запрет, на всех клиентских устройствах используется одно и то же заданное политикой значение.

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

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

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

- политикой группы, если в политике был установлен запрет на изменение параметра.

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

Точка распространения

Точка распространения (ранее называлась "агент обновлений") – это устройство с установленным Агентом администрирования, который используется для распространения обновлений, удаленной установки приложений, получения информации об устройствах в сети. Точки распространения ускоряют распространение обновлений и позволяют высвободить ресурсы Сервера 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 файлы, полученные от Сервера администрирования, на клиентские устройства группы (в том числе с помощью широковещательной рассылки по протоколу UDP).

  Список файлов, которые могут быть переданы точками распространения, включает:

  - Базы и модули приложений "Лаборатории Касперского".
  - Обновления приложений сторонних производителей.
  - Инсталляционные пакеты.
  - Обновления Windows, если вы используете Сервер администрирования в роли WSUS-сервера.

  Обновления могут быть получены как с Сервера администрирования, так и с серверов обновлений "Лаборатории Касперского". В последнем случае для точки распространения должна быть создана задача обновления. Точки распространения 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.

  Если все точки распространения, назначенные устройству, неисправны, устройство не будет получать обновления (антивирусные базы и патчи) и инсталляционные пакеты.

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

- Выполнять роль шлюза соединений с Сервером администрирования для устройств группы администрирования.

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

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

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

- Выполнять удаленную установку приложений сторонних производителей и приложений "Лаборатории Касперского" средствами операционной системы точки распространения. Обратите внимание, что точка распространения может выполнять установку на клиентские устройства без Агента администрирования.

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

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

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

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

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

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

Областью действия точек распространения также может являться сетевое местоположение. Сетевое местоположение используется для формирования вручную набора устройств, на которые точка распространения будет распространять обновления. Определение сетевого местоположения доступно только для устройств под управлением операционной системы Windows.

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

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

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

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

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

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

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

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

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

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

Шлюз соединения

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

Шлюз соединения может принимать соединения от 10 000 устройств.

Существует два варианта использования шлюзов соединения:

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

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

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

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

- Вы также можете использовать шлюзы соединения в сети. Например, автоматически назначаемые точки распространения также становятся шлюзами соединения в своей области действия. Однако во внутренней сети шлюзы соединения не дают значительных преимуществ. Они уменьшают количество сетевых подключений, принимаемых Сервером администрирования, но не уменьшают объем входящих данных. Даже без шлюзов соединения все устройства могли подключаться к Серверу администрирования.

Основной сценарий установки

Следуя основному сценарию, вы можете развернуть Сервер администрирования, а также установить на устройства сети Агент администрирования и приложения безопасности. Вы можете использовать этот сценарий и для ознакомления с приложением, и для установки приложения с целью дальнейшей работы.

Установка Kaspersky Security Center включает следующие шаги:

1. Подготовка.

2. Установка Kaspersky Security Center и приложений безопасности "Лаборатории Касперского" на устройстве с Сервером администрирования

3. Удаленное развертывание приложений безопасности "Лаборатории Касперского" на клиентских устройствах.

Развертывание Kaspersky Security Center в облачном окружении и развертывание Kaspersky Security Center для поставщиков услуг описаны в соответствующих разделах справки.

Рекомендуется отвести на установку Сервера администрирования не менее часа, а на выполнение сценария целиком – не менее одного рабочего дня. На устройство, которое будет выполнять роль Сервера администрирования Kaspersky Security Center, также рекомендуется установить приложение безопасности, например, Kaspersky Security для Windows Server или Kaspersky Endpoint Security.

После завершения сценария в сети организации будет развернута защита из следующим способом:

- Для Сервера администрирования будет установлена СУБД.
- Сервер администрирования Kaspersky Security Center будет установлен.
- Все необходимые политики и задачи будут созданы, а также будут настроены заданные по умолчанию параметры политик и задач.
- На управляемые устройства будут установлены приложения безопасности (например, Kaspersky Endpoint Security для Windows) и Агент администрирования.
- Группы администрирования будут созданы (возможно, объединенные в иерархию).
- При необходимости будет развернута защита мобильных устройств.
- При необходимости будут назначены точки распространения.

Установка Kaspersky Security Center происходит поэтапно:

Подготовка

1. **Получение необходимых файлов**

   Убедитесь, что у вас есть лицензионный ключ (код активации) для Kaspersky Security Center или лицензионные ключи (коды активации) для приложений безопасности "Лаборатории Касперского".

   Распакуйте архив, полученный от вашего поставщика. Этот архив содержит лицензионные ключи (файлы формата KEY), коды активации и список приложений "Лаборатории Касперского", которые могут быть активированы каждым из этих лицензионных ключей.

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

   Подробную информацию о лицензировании приложений безопасности "Лаборатории Касперского", которые не входят в состав Kaspersky Security Center, вы можете найти в документации к этим приложениям.

2. **Выбор структуры защиты организации**

   Ознакомьтесь с компонентами Kaspersky Security Center. Выберите структуру защиты и конфигурацию сети, наиболее подходящие для вашей организации. Исходя из конфигурации сети и пропускной способности каналов связи определите, какое количество Серверов администрирования необходимо использовать и как их разместить по офисам, если вы работаете с распределенной сетью.

   Для достижения и сохранения оптимальной производительности при различных условиях работы, пожалуйста, учитывайте количество устройств в сети, топологию сети и необходимый вам набор функций Kaspersky Security Center (подробнее см. в Руководстве по масштабированию Kaspersky Security Center).

   Определите, будет ли в вашей организации использоваться иерархия Серверов администрирования. Для этого нужно понять, возможно и целесообразно ли обслуживание всех клиентских устройств одним Сервером администрирования или требуется выстроить иерархию Серверов администрирования. Вам также может потребоваться выстроить иерархию Серверов администрирования, совпадающую с организационной структурой предприятия, сеть которого вы хотите защитить.

   Если вам требуется обеспечить защиту мобильных устройств, выполните подготовительные действия по настройке Сервера iOS MDM.

Убедитесь, что устройства, выбранные вами для использования в качестве Серверов администрирования, а также для установки Консоли администрирования, соответствуют аппаратным и программным требованиям.

3. **Подготовка к использованию пользовательских сертификатов**

Если инфраструктура открытых ключей (PKI) вашей организации требует, чтобы вы использовали пользовательские сертификаты, выпущенные определенным доверенным центром сертификации (CA), подготовьте эти сертификаты и убедитесь, что они соответствуют всем требованиям.

4. **Подготовка к лицензированию Kaspersky Security Center**

Если вы планируете использовать версию Kaspersky Security Center с поддержкой Управления мобильными устройствами, Интеграцией с SIEM-системами и / или с поддержкой Системного администрирования, убедитесь, что у вас имеется файл ключа либо код активации для лицензирования приложения.

5. **Подготовка к лицензированию управляемых приложений безопасности**

Во время развертывания защиты вам потребуется предоставить "Лаборатории Касперского" активные лицензионные ключи на те приложения, которыми вы планируете управлять с помощью Kaspersky Security Center (см. список доступных для управления приложений безопасности). Подробнее о лицензировании каждого из приложений безопасности вы можете прочитать в документации к этим приложениям.

6. **Выбор аппаратной конфигурации Сервера администрирования и СУБД**

Спланируйте аппаратную конфигурацию для СУБД и Сервера администрирования с учетом количества устройств в вашей сети.

7. **Выбор СУБД**

При выборе СУБД учитывайте количество управляемых устройств, которые будет обслуживать Сервер администрирования. Если в вашей сети менее 10 000 устройств и вы не планируете увеличивать их количество, вы можете выбрать бесплатную СУБД SQL Express или MySQL и установить ее на одном устройстве с Сервером администрирования. Вы можете выбрать СУБД MariaDB, которая позволяет управлять устройствами в количестве до 20 000. Если в вашей сети более 10 000 устройств (или вы планируете расширение сети до такого количества устройств), рекомендуется выбирать платную СУБД SQL и размещать ее на отдельном устройстве. Платная СУБД может работать с несколькими Серверами администрирования, а бесплатная СУБД – только с одним.

Если вы выберете SQL Server, тогда можно перенести данные, хранящиеся в базе данных, в MySQL, в MariaDB или в Azure SQL СУБД. Чтобы выполнить перенос данных, выполните резервное копирование данных и восстановите их в новой СУБД.

> Если вы выбрали MSSQL 2019, вам нужно использовать накопительное исправление CU12 или выше. Чтобы избежать ошибки и перегрузки системы, которая может возникнуть.

8. **Установка СУБД и создание базы данных**

Узнайте больше об учетных записях для работы с СУБД и установите СУБД.

Перед установкой выберите поддерживаемую СУБД. Вы можете выбрать, например, PostgreSQL, Postgres Pro, Microsoft SQL Server, MySQL или MariaDB.

Подробнее о том как установить выбранную СУБД, см. в документации к этой СУБД.

Если вы установите MariaDB, MySQL, PostgreSQL или Postgres Pro используйте рекомендуемые параметры, чтобы обеспечить правильную работу СУБД.

Запишите и сохраните параметры СУБД, поскольку они потребуются вам при установке Сервера администрирования. Эти параметры включают имя SQL-сервера, номер порта для подключения к SQL-серверу, имя учетной записи и пароль для доступа к SQL-серверу.

Если вы решили установить СУБД PostgreSQL или Postgres Pro, убедитесь, что вы указали пароль для суперпользователя. Если пароль не указан, Сервер администрирования может не подключиться к базе данных.

По умолчанию инсталлятор Kaspersky Security Center создает базу данных для размещения информации Сервера администрирования, однако вы можете отказаться от ее создания и использовать другую базу данных. В этом случае убедитесь, что база данных создана, вы знаете ее имя, а учетная запись, под которой Сервер администрирования получит доступ к этой базе данных, будет иметь для нее роль db_owner.

При необходимости обратитесь за информацией к администратору СУБД.

9. **Настройка портов**

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

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

10. **Проверка учетных записей**

    Проверьте наличие у вас прав локального администратора для успешной установки Сервера администрирования Kaspersky Security Center и развертывания защиты на устройствах. Права локального администратора на клиентских устройствах нужны для установки на эти устройства Агента администрирования. После установки Агента администрирования вы сможете с его помощью удаленно устанавливать приложения на устройства, не пользуясь учетной записью с правами администратора устройства.

    По умолчанию инсталлятор Kaspersky Security Center создает на устройстве, выбранном для установки Сервера администрирования, три локальные учетные записи, от имени которых будет запускаться Сервер администрирования и службы Kaspersky Security Center:

    - KL-AK-*: учетная запись службы Сервера администрирования;
    - NT Service/KSC*: учетная запись для прочих служб из состава Сервера администрирования;
    - KlPxeUser: учетная запись для развертывания операционных систем.

    Вы можете отказаться от создания учетных записей для служб Сервера администрирования и других служб. Вместо этого вы можете использовать существующие учетные записи, например учетные записи домена, если планируете установить Сервер администрирования на отказоустойчивом кластере или планируете использовать учетные записи домена вместо локальных учетных записей по другой причине. В этом случае убедитесь, что учетные записи для запуска Сервера администрирования и сервисов Kaspersky Security Center созданы, являются непривилегированными и обладают необходимыми правами для доступа к СУБД. (Если вы планируете в дальнейшем разворачивать операционные системы на устройствах средствами Kaspersky Security Center, не отказывайтесь от создания учетных записей.)

Установка Kaspersky Security Center и приложений безопасности "Лаборатории Касперского" на устройстве с Сервером администрирования

1. **Установка Сервера администрирования, Консоли администрирования, Kaspersky Security Center Web Console и плагинов управления для приложений безопасности**

   Загрузите Kaspersky Security Center с сайта "Лаборатории Касперского". Можно загрузить полный пакет, только Kaspersky Security Center Web Console или только Консоль администрирования.

Установите Сервер администрирования на устройство, которое вы выбрали (либо устройства, если вы планируете использовать более одного Сервера администрирования). Вы можете выбрать стандартную или выборочную установку Сервера администрирования. Вместе с Сервером администрирования установится Консоль администрирования. Рекомендуется устанавливать Сервер администрирования на выделенный сервер, а не на контроллер домена.

Стандартная установка – это рекомендуется, если вы хотите ознакомиться с приложением Kaspersky Security Center, например протестировать его работу на небольшом участке сети вашей организации. При стандартной установке вы настраиваете только параметры базы данных. Также вы можете установить только набор плагинов управления, заданный по умолчанию, для приложений "Лаборатории Касперского". Вы также можете воспользоваться стандартной установкой, если вы уже имеете опыт работы с Kaspersky Security Center и знаете, как после стандартной установки настроить все необходимые вам параметры.

Выборочная установка – это рекомендуется, если вы планируете настроить параметры Kaspersky Security Center, такие как путь к папке общего доступа, учетные записи и порты подключения к Серверу администрирования, а также параметры базы данных. Выборочная установка позволяет указать, какие плагины управления приложениями "Лаборатории Касперского" будут установлены. При необходимости вы можете запустить выборочную установку в тихом режиме.

Вместе с Сервером администрирования устанавливаются также Консоль администрирования и серверная версия Агента администрирования. Можно также выбрать установку Kaspersky Security Center Web Console.

При необходимости можно установить Консоль администрирования и Kaspersky Security Center Web Console на рабочее место администратора независимо для управления Сервером администрирования по сети.

2 Первоначальная настройка и лицензирование

После завершения установки Сервера администрирования при первом подключении к Серверу администрирования автоматически запускается Мастер первоначальной настройки. Выполните первоначальную настройку Сервера администрирования в соответствии с вашими требованиями. На этапе первоначальной настройки мастер создает необходимые для развертывания защиты политики и задачи с параметрами по умолчанию. Эти параметры могут оказаться неоптимальными для нужд вашей организации. При необходимости вы можете изменить параметры политик и задач (Настройка защиты в сети организации-клиента, Сценарий: настройка защиты сети).

Если вы планируете использовать функциональность, выходящую за рамки Базовой функциональности, активируйте приложение по лицензии. Вы можете выполнить это на одном из шагов мастера первоначальной настройки.

3 Проверка успешности установки Сервера администрирования

После успешного выполнения предыдущих шагов Сервер администрирования установлен и готов к дальнейшей работе.

Убедитесь, что работает Консоль администрирования и что вы можете подключиться через Консоль к Серверу администрирования. Убедитесь также, что на Сервере администрирования имеется задача загрузки обновлений в хранилище Сервера администрирования (в папке **Задачи** дерева консоли) и политика для Kaspersky Endpoint Security (в папке **Политики** дерева консоли).

После завершения проверки, перейдите к шагам ниже.

Удаленное развертывание приложений безопасности "Лаборатории Касперского" на клиентских устройствах

1. **Обнаружение устройств в сети**

   Этот шаг входит в мастер первоначальной настройки. Вы можете также запустить обнаружение устройств вручную. В результате Сервер администрирования Kaspersky Security Center получает адреса и имена всех устройств, зарегистрированных в сети. В дальнейшем вы можете с помощью Kaspersky Security Center устанавливать приложения "Лаборатории Касперского" и других производителей на обнаруженные устройства. Kaspersky Security Center запускает обнаружение устройств регулярно, поэтому, если в сети появятся новые устройства, они будут обнаружены автоматически.

2. **Установка Агента администрирования и приложений безопасности на устройства в сети**

   Развертывание защиты (Настройка защиты в сети организации-клиента, Сценарий: настройка защиты сети) в сети организации подразумевает установку Агента администрирования и приложений безопасности (например, Kaspersky Endpoint Security) на устройства, найденные Сервером администрирования в процессе обнаружения устройств.

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

   При необходимости можно установить Агент администрирования в тихом режиме с файлом ответов или без него.

   Перед тем как установить Агент администрирования и приложения безопасности на устройства в сети, убедитесь, что эти устройства доступны (то есть включены). Вы можете установить Агент администрирования на виртуальные машины, так же как и на физические устройства.

   Возможна удаленная или локальная установка приложений безопасности и Агента администрирования.

   Удаленная установка – с помощью мастера развертывания защиты вы можете удаленно установить приложение безопасности (например, Kaspersky Endpoint Security для Windows) и Агент администрирования на устройствах, которые были обнаружены Сервером администрирования в сети организации. Как правило, задача удаленной установки успешно развертывает защиту для большинства сетевых устройств. Однако она может возвращать ошибку на некоторых устройствах, если, например, устройство отключено или недоступно по другой причине. В этом случае рекомендуется вручную подключиться к устройству и использовать локальную установку.

   Локальная установка – используется на тех устройствах сети, на которых не удалось развернуть защиту с помощью задачи удаленной установки. Чтобы установить защиту на такие устройства, создайте автономный инсталляционный пакет для запуска на этих устройствах локально.

   Установка Агента администрирования на устройства с операционными системами Linux и macOS описана в документации для Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Mac соответственно. Несмотря на то, что устройства под управлением операционных систем Linux и macOS считаются менее уязвимыми, чем устройства под управлением Windows, на них также рекомендуется устанавливать приложения безопасности.

   После установки убедитесь, что приложение безопасности установлено на управляемые устройства. Для этого запустите Отчет о версиях приложений "Лаборатории Касперского" и ознакомьтесь с его результатами.

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

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

4. **Настройка защиты мобильных устройств**

   Этот шаг входит в мастер первоначальной настройки.

   Чтобы управлять корпоративными мобильными устройствами, выполните необходимые подготовительные шаги и разверните Управление мобильными устройствами.

5. **Создание структуры групп администрирования**

   В некоторых случаях для развертывания защиты на устройствах сети оптимальным образом может потребоваться разделить устройства на группы администрирования с учетом организационной структуры организации. Вы можете создать правила перемещения для распределения устройств по группам или распределить устройства вручную. Для групп администрирования можно назначать групповые задачи, определять область действия политик и назначать точки распространения.

   Убедитесь, что все управляемые устройства правильно распределены по соответствующим группам администрирования и что у вас в сети не осталось нераспределенных устройств.

6. **Назначение точек распространения**

   Kaspersky Security Center автоматически назначает точки распространения группам администрирования, но при необходимости вы можете назначить их вручную. Точки распространения рекомендуется использовать в больших сетях для снижения нагрузки на Сервер администрирования, а также в сетях с распределенной структурой для предоставления Серверу администрирования доступа к устройствам или группам устройств, соединенным каналами с низкой пропускной способностью. В качестве точек распространения можно использовать устройства под управлением Linux и под управлением Windows.

Порты, используемые Kaspersky Security Center

В таблицах ниже показаны порты по умолчанию, используемые Серверами администрирования и клиентскими устройствами. Если вы хотите, вы можете изменить номера портов по умолчанию.

Если Сервер администрирования и база данных установлены на разные устройства, необходимо сделать доступными необходимые порты на устройстве с базой данных (например, порт 3306 для MySQL Server, порт 1433 для Microsoft SQL Server или порт 5432 для PostgreSQL и Postgres Pro). Подробную информацию см. в документации СУБД.

Порты, используемые Сервером администрирования

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
8060	klcsweb	TCP	Передача на клиентские устройства опубликованных инсталляционных пакетов	Публикация инсталляционных пакетов. Вы можете изменить номер порта по умолчанию в разделе **Веб-сервер** окна свойств Сервера администрирования в Консоли администрирования или в Kaspersky Security Center Web Console. Этот порт является необязательным. В целях безопасности рекомендуется использовать TCP-порт 8061.
8061	klcsweb	TCP (TLS)	Передача на клиентские устройства опубликованных инсталляционных пакетов	Публикация инсталляционных пакетов. Вы можете изменить номер порта по умолчанию в разделе **Веб-сервер** окна свойств Сервера администрирования в Консоли администрирования или в Kaspersky Security Center Web Console.

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
13000	klserver	TCP (TLS)	Прием подключений от Агентов администрирования и от подчиненных Серверов администрирования; используется также на подчиненных серверах для приема подключений от главного Сервера (например, если подчиненный Сервер находится в демилитаризованной зоне)	Управление клиентскими устройствами и подчиненными Серверами администрирования. Вы можете изменить номер порта по умолчанию для приема подключений от Агентов администрирования при настройке портов подключения. Вы можете изменить номер порта по умолчанию для приема подключений от подчиненных Серверов администрирования при создании иерархии Серверов администрирования в Консоли администрирования или в Kaspersky Security Center Web Console.
13000	klserver	UDP	Прием информации от Агентов администрирования о выключении устройств	Управление клиентскими устройствами. Вы можете изменить номер порта по умолчанию в параметрах политики Агента администрирования в Консоли администрирования или в Kaspersky Security Center Web Console.
13291	klserver	TCP (TLS)	Прием подключений от Консоли администрирования к Серверу администрирования	Управление Сервером администрирования. Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования в Консоли администрирования.
13299	klserver	TCP (TLS)	Прием подключений от Kaspersky Security Center Web Console к Серверу администрирования; прием подключений к Серверу администрирования через OpenAPI	Kaspersky Security Center Web Console, OpenAPI. Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования (раздел **Параметры подключения к Серверу администрирования** → подраздел **Порты подключения**) в Консоли администрирования на основе консоли Microsoft Management Console (MMC), либо при создании иерархии Серверов администрирования в Консоли администрирования или в Kaspersky Security Center Web Console.
14000	klserver	TCP	Прием подключений от Агентов администрирования	Управление клиентскими устройствами. Вы можете изменить номер порта по умолчанию при настройке портов подключения при установке Kaspersky Security Center или при подключении клиентского устройства к Серверу администрирования вручную. Этот порт является необязательным. В целях безопасности рекомендуется использовать TCP-порт 13000.
13111 (только если на устройстве запущена служба прокси-сервера KSN)	ksnproxy	TCP	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN. Вы можете изменить значения портов по умолчанию в окне свойств Сервера администрирования.
15111 (только если на устройстве запущена служба прокси-сервера KSN)	ksnproxy	UDP	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN. Вы можете изменить значения портов по умолчанию в окне свойств Сервера администрирования.
17000	klactprx	TCP (TLS)	Прием подключений для активации приложений от управляемых устройств (кроме мобильных устройств)	Прокси-сервер активации, используемый немобильными устройствами для активации приложений "Лаборатории Касперского" с помощью кодов активации. Вы можете изменить значения портов по умолчанию в окне свойств Сервера администрирования.
17100 (только если вы управляете мобильными устройствами)	klactprx	TCP (TLS)	Прием подключений для активации приложений от мобильных устройств	Прокси-сервер активации для мобильных устройств. Вы можете изменить значения портов по умолчанию в окне свойств Сервера администрирования.

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
19170	klserver	HTTPS (TLS)	Туннелирование соединения с управляемыми устройствами с помощью утилиты klsctunnel	Удаленное подключение к управляемым устройствам с помощью Kaspersky Security Center Web Console. Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования (в разделе **Параметры подключения к Серверу администрирования** → подразделе **Порты подключения** → **Открыть RDP-порт для Kaspersky Security Center Web Console**) только в Консоли администрирования.
13292 (только если вы управляете мобильными устройствами)	klserver	TCP (TLS)	Прием подключений от мобильных устройств	Управление мобильными устройствами. Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования в Консоли администрирования или в Kaspersky Security Center Web Console.
13294 (только если вы управляете мобильными устройствами)	klserver	TCP (TLS)	Прием подключений от устройств с защитой на уровне UEFI	Управление клиентскими устройствами с защитой на уровне UEFI. Вы можете изменить номер порта по умолчанию при подключении мобильных устройств или позже в окне свойств Сервера администрирования (в подразделе **Порты подключения** раздела (**Параметры подключения к Серверу администрирования**) в Консоли администрирования или в Kaspersky Security Center Web Console.
13296	klserver	TCP (TLS)	Публикация метрик Kaspersky Security Center для Prometheus	Публикация метрик Kaspersky Security Center, которые в дальнейшем получит Prometheus. Посмотреть метрики можно по ссылке: https://<адрес_сервера>:13296/metrics. В поле <адрес_сервера> укажите IP-адрес или доменное имя вашего Сервера администрирования. Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования в Консоли администрирования.
30522, 30523 (порты в интерфейсе localhost)	klnagent	TCP	Перенос обновлений приложений из Агента администрирования в локально установленные приложения "Лаборатории Касперского" с помощью компонента FileTransferBridge.	Устройство Сервера администрирования, которое получает обновления приложений "Лаборатории Касперского".

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

Порт, используемый Сервером iOS MDM

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

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

Порт, используемый Сервером Kaspersky Security Center Web Console

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

В таблице ниже указан порт, который используется управляемыми устройствами с установленным Агентом администрирования.

Порты, используемые Агентом администрирования

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
15000	klnagent	UDP	Сигналы управления от Сервера администрирования или точки распространения к Агентам администрирования	Управление клиентскими устройствами. Вы можете изменить номер порта по умолчанию в параметрах политики Агента администрирования в Консоли администрирования или в Kaspersky Security Center Web Console.
15000	klnagent	Широковещательная рассылка UDP	Получение данных о других Агентах администрирования в том же широковещательном домене (далее данные отправляются на Сервер администрирования)	Доставка обновлений и инсталляционных пакетов.
15001	klnagent	UDP	Получение многоадресных запросов от точек распространения (если используется)	Получение обновлений и инсталляционных пакетов от точки распространения. Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования или в Kaspersky Security Center Web Console.
30522, 30523 (порты в интерфейсе localhost)	klnagent	TCP	Получение обновлений приложений "Лаборатории Касперского" с Сервера администрирования с помощью компонента FileTransferBridge	Управляемые устройства, которые получают обновления приложения "Лаборатории Касперского" с Сервера администрирования, указанного в качестве источника обновлений баз.
161	klnagent	SNMP	Мониторинг и обнаружение сетевых устройств	Обнаружение устройств.

Обратите внимание, что процесс klnagent также может запрашивать свободные порты из динамического диапазона портов операционной системы конечного устройства. Операционная система назначает эти порты процессу klnagent автоматически, поэтому процесс klnagent может использовать некоторые порты, используемые другим программным обеспечением. Если процесс klnagent влияет на работу этого программного обеспечения, измените параметры порта в программном обеспечении или измените динамический диапазон портов по умолчанию в вашей операционной системе, чтобы исключить порт, используемый этим программным обеспечением.

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

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

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

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
13000	klnagent	TCP (TLS)	Прием подключений от Агентов администрирования и от Kaspersky Security Center когда точка распространения выполняет роль шлюза соединения в демилитаризованной зоне. Если в качестве точки распространения указано устройство с установленным Сервером администрирования, для SSL-соединения по умолчанию используется порт 13001 вместо 13000.	Управление клиентскими устройствами, доставка обновлений и инсталляционных пакетов. Подробнее см. в раздел: Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство. Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования или в Kaspersky Security Center Web Console.
13111 (только если на устройстве запущена служба прокси-сервера KSN)	ksnproxy	TCP	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN. Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования или в Kaspersky Security Center Web Console.
15111 (только если на устройстве запущена служба прокси-сервера KSN)	ksnproxy	UDP	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN. Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования или в Kaspersky Security Center Web Console.
17111 (только если на устройстве запущена служба прокси-сервера KSN)	ksnproxy	HTTPS	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN. Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования или в Kaspersky Security Center Web Console.
13295 (только если вы используете точку распространения в качестве push-сервера)	klnagent	TCP (TLS)	Прием подключений от клиентских устройств	Push-сервер. Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования или в Kaspersky Security Center Web Console.

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

Порты, используемые на устройстве контроллера домена

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

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

Порт, используемый на нераспределенном клиентском устройстве

Номер порта	Протокол	Назначение порта	Область
22	SSH	Подключение к клиентскому устройству по протоколу SSH	Только для клиентских устройств с операционными системами Linux. Удаленная установка приложений "Лаборатории Касперского" с помощью точки распространения с операционной системой Linux.

Сертификаты для работы с Kaspersky Security Center

Этот раздел содержит информацию о сертификатах Kaspersky Security Center и описывает, как выпустить пользовательский сертификат для Сервера администрирования.

О сертификатах Kaspersky Security Center

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

- Сертификат Сервера администрирования.
- Мобильный сертификат.
- Сертификат Сервера iOS MDM.
- Сертификат Веб-сервера Kaspersky Security Center.
- Сертификат Kaspersky Security Center Web Console.

По умолчанию Kaspersky Security Center использует самоподписанные сертификаты (то есть выданные самим Kaspersky Security Center). Если требуется, вы можете заменить самоподписанные сертификаты пользовательскими сертификатами, в соответствии со стандартами безопасности вашей организации. После того как Сервер администрирования проверит соответствие пользовательского сертификата всем применимым требованиям, этот сертификат приобретает такую же область действия, что и самоподписанный сертификат. Единственное отличие состоит в том, что пользовательский сертификат не перевыпускается автоматически по истечении срока действия. Вы заменяете сертификаты на пользовательские с помощью утилиты klsetsrvcert или в Консоли администрирования в свойствах Сервера администрирования, в зависимости от типа сертификата. При использовании утилиты klsetsrvcert необходимо указать тип сертификата, используя одно из следующих значений:

- C – общий сертификат для портов 13000 и 13291.
- CR – общий резервный сертификат для портов 13000 и 13291.
- M – мобильный сертификат для порта 13292.

- MR – мобильный резервный сертификат для порта 13292.
- MCA – мобильный сертификат, полученный от аккредитованного центра сертификации для автоматической генерации пользовательских сертификатов.

Вам не нужно загружать утилиту klsetsrvcert. Утилита входит в состав комплекта поставки Kaspersky Security Center. Утилита несовместима с предыдущими версиями Kaspersky Security Center.

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

Сертификаты Сервера администрирования

Сертификат Сервера администрирования необходим для аутентификации Сервера администрирования, а также для безопасного взаимодействия Сервера администрирования и Агента администрирования на управляемых устройствах или между главным Сервером администрирования и подчиненными Серверами. При первом подключении Консоли администрирования к Серверу администрирования вам будет предложено подтвердить использование текущего сертификата Сервера администрирования. Такое подтверждение также требуется при каждой замене сертификата Сервера администрирования, после каждой переустановки Сервера администрирования и при подключении подчиненного Сервера администрирования к главному Серверу администрирования. Этот сертификат называется общим ("C").

Общий сертификат ("C") создается автоматически при установке компонента Сервера администрирования. Сертификат состоит из двух частей:

- Файл klserver.cer; по умолчанию он находится на устройстве, на котором установлен компонент Сервера администрирования, в папке C:\ProgramData\KasperskyLab\adminkit\1093\cert.
- Секретный ключ находится в защищенном хранилище Windows (Windows Protected Storage).

Также существует общий резервный сертификат ("CR"). Kaspersky Security Center автоматически генерирует этот сертификат за 90 дней до истечения срока действия общего сертификата. Общий резервный сертификат впоследствии используется для замены сертификата Сервера администрирования. Когда истекает срок действия общего сертификата, общий резервный сертификат используется для поддержания связи с экземплярами Агента администрирования, установленными на управляемых устройствах. С этой целью общий резервный сертификат автоматически становится новым общим сертификатом за 24 часа до истечения срока действия старого общего сертификата.

Вы также можете создать резервную копию сертификата Сервера администрирования отдельно от других параметров Сервера администрирования, чтобы перенести Сервер администрирования с одного устройства на другое без потери данных.

Мобильные сертификаты

Мобильный сертификат ("M") необходим для аутентификации Сервера администрирования на мобильных устройствах. Вы настраиваете использование мобильного сертификата на шаге мастера первоначальной настройки.

Также существует мобильный резервный сертификат ("MR"): он используется для замены мобильного сертификата. Kaspersky Security Center автоматически генерирует этот сертификат за 90 дней до истечения срока действия общего сертификата. Когда истекает срок действия мобильного сертификата, мобильный резервный сертификат используется для поддержания связи с Агентами администрирования, установленными на управляемых мобильных устройствах. С этой целью мобильный резервный сертификат автоматически становится новым мобильным сертификатом за 24 часа до истечения срока действия старого мобильного сертификата.

Если сценарий подключения требует использования сертификата клиента на мобильных устройствах (подключение с двусторонней SSL-аутентификация), вы генерируете эти сертификаты с помощью доверенного центра сертификации для автоматически сгенерированных пользовательских сертификатов ("MCA"). Кроме того, мастер первоначальной настройки позволяет вам начать использовать пользовательские сертификаты, выпущенные другим доверенного центром сертификации, а интеграция с инфраструктурой открытых ключей (PKI) вашей организации позволяет выпускать сертификаты клиентов с помощью центра сертификации домена.

Сертификат Сервера iOS MDM

Сертификат Сервера iOS MDM необходим для аутентификации Сервера администрирования на мобильных устройствах под управлением операционной системы iOS. Взаимодействие с этими устройствами осуществляется через протокол Apple Mobile Device Management (MDM), в котором не используется Агент администрирования. Вместо этого вы устанавливаете специальный iOS MDM-профиль, содержащий клиентский сертификат, на каждом устройстве, чтобы обеспечить двустороннюю SSL-аутентификацию.

Кроме того, мастер первоначальной настройки позволяет вам начать использовать пользовательские сертификаты, выпущенные другим доверенного центром сертификации, а интеграция с инфраструктурой открытых ключей (PKI) вашей организации позволяет выпускать сертификаты клиентов с помощью центра сертификации домена.

Клиентские сертификаты передаются на устройства iOS, когда вы загружаете эти iOS MDM-профили. Пользовательский сертификат Сервера iOS MDM уникален для каждого управляемого устройства iOS. Вы генерируете все клиентские сертификаты Сервера iOS MDM с помощью аккредитованного центра сертификации для автоматически сгенерированных пользовательских сертификатов ("MCA").

Сертификат Веб-сервера Kaspersky Security Center

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

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

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

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

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

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

Сертификат Kaspersky Security Center Web Console

Сервер Kaspersky Security Center Web Console (далее также Web Console) имеет собственный сертификат. Когда вы открываете сайт, браузер проверяет, является ли ваше соединение надежным. Сертификат Web Console позволяет аутентифицировать Web Console и используется для шифрования трафика между браузером и Web Console.

Когда вы открываете Web Console, браузер может информировать вас о том, что подключение к Web Console не является приватным и что сертификат Web Console недействителен. Это предупреждение появляется потому, что сертификат Kaspersky Security Center Web Console является самоподписанным и автоматически генерируется Kaspersky Security Center. Чтобы удалить это предупреждение, можно выполнить одно из следующих действий:

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

О сертификате Сервера администрирования

Выполняются две операции с использованием *сертификата Сервера администрирования:* аутентификация Сервера администрирования при подключении Консоли администрирования и обмен данными с устройствами. Сертификат используется также для аутентификации, когда главные Серверы администрирования подключены к подчиненным Серверам администрирования.

Сертификаты, выписанные "Лабораторией Касперского"

Сертификат Сервера администрирования автоматически создается при установке компонента Сервер администрирования и хранится в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

Сертификат Сервера администрирования действителен в течение пяти лет, если сертификат был сгенерирован Сервером администрирования версии 12.2 или более ранней. В противном случае срок действия сертификата ограничен 397 днями. Новый сертификат генерируется Сервером администрирования как резервный сертификат, за 90 дней до срока окончания действия текущего сертификата. Затем новый сертификат автоматически замещает текущий сертификат за один день до окончания его срока действия. Все Агенты администрирования на клиентских устройствах автоматически настраиваются на аутентификацию с Сервером администрирования с использованием нового сертификата.

Пользовательские сертификаты

При необходимости можно назначить Серверу администрирования пользовательский сертификат. Например, это может понадобиться для лучшей интеграции с существующей PKI вашей организации или для требуемой настройки полей сертификата.

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

При замене сертификата все Агенты администрирования, ранее подключенные к Серверу администрирования по SSL, перестанут подключаться к Серверу с ошибкой "Ошибка аутентификации Сервера администрирования". Чтобы устранить эту ошибку, вам потребуется восстановить соединение после замены сертификата.

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

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

Требования к пользовательским сертификатам, используемым в Kaspersky Security Center

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

Тип сертификата	Требования	Комментарии
Общий сертификат, Общий резервный сертификат ("C", "CR")	Минимальная длина ключа: 2048. Основные ограничения: • Ограничение длины пути: Отсутствует. Использование ключа: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (Extended Key Usage, EKU) (необязательно): аутентификация сервера, аутентификация клиента. Сертификат должен включать допустимое альтернативное имя субъекта (Subject Alternative Name, SAN), которое содержит адрес Сервера администрирования для обратной связи: • Для IPv4: 127.0.0.1 • Для IPv6: 0:0:0:0:0:0:0:1	Параметр Extended Key Usage является необязательным. Значение ограничения длины пути может быть целым числом, отличным от "None", но не должно быть меньше 1.
Мобильный сертификат, Мобильный резервный сертификат ("M", "MR")	Минимальная длина ключа: 2048. Основные ограничения: • CA: Да. • Ограничение длины пути: Отсутствует. Использование ключа: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (EKU) (необязательно): аутентификация Сервера.	Параметр Extended Key Usage является необязательным. Значение ограничения длины пути может быть целым числом, отличным от "None", если Общий сертификат имеет значение ограничения длины пути не менее 1.
Сертификат, выпущенный доверенным центром сертификации (CA), для автоматически генерируемых пользовательских сертификатов (MCA)	Минимальная длина ключа: 2048. Основные ограничения: • CA: Да. • Ограничение длины пути: Отсутствует. Использование ключа: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (Extended Key Usage, EKU) (необязательно): аутентификация сервера, аутентификация клиента.	Параметр Extended Key Usage является необязательным. Значение ограничения длины пути может быть целым числом отличным от "None", если Общий сертификат имеет значение ограничения длины пути не менее 1.
Сертификат Веб-сервера	Расширенное использование ключа (EKU): аутентификация сервера. Контейнер PKCS #12 / PEM, из которого указывается сертификат, включает всю цепочку открытых ключей. Присутствует альтернативное имя субъекта (SAN) сертификата; то есть значение поля `subjectAltName` является допустимым. Сертификат соответствует действующим требованиям браузеров, предъявляемым к сертификатам серверов, а также к текущим базовым требованиям CA/Browser Forum.	—

Тип сертификата	Требования	Комментарии
Сертификат Kaspersky Security Center Web Console	Контейнер PEM, из которого указывается сертификат, включает всю цепочку открытых ключей. Присутствует альтернативное имя субъекта (SAN) сертификата; то есть значение поля `subjectAltName` является допустимым. Сертификат соответствует действующим требованиям браузеров к сертификатам серверов, а также к текущим базовым требованиям CA/Browser Forum.	Зашифрованные сертификаты не поддерживаются Kaspersky Security Center Web Console.

Сценарий: задание пользовательского сертификата Сервера администрирования

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

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

Предварительные требования

Должны быть соблюдены следующие условия:

- Сертификат должен быть создан в формате PKCS#12 (например, с помощью PKI организации).
- Для нового сертификата должны быть соблюдены требования, перечисленные в таблице ниже.

  В таблице ниже обратите внимание на требование "CA: true". Оно означает, что новый сертификат должен быть выдан доверенным центром сертификации (CA). Новый сертификат с требованием "CA: true" должен включать в себя всю цепочку доверия и закрытый ключ, который должен храниться в файле с расширением pfx или p12.

Тип сертификата	Требования
Общий сертификат, общий резервный сертификат ("C", "CR")	Минимальная длина ключа: 2048. Основные ограничения: • Ограничение длины пути: Отсутствует. Значение ограничения длины пути может быть целым числом отличным от "None", но не меньше 1. Использование ключа: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (Extended Key Usage, EKU) (необязательно): аутентификация сервера и аутентификация клиента. EKU необязательно, но если оно содержится в вашем сертификате, данные аутентификации сервера и клиента должны быть указаны в EKU. Сертификат должен содержать действительное альтернативное имя субъекта (SAN). В поле `subjectAltName` должен быть указан loopback-адрес Сервера администрирования: • Для IPv4: 127.0.0.1 • Для IPv6: 0:0:0:0:0:0:0:1
Мобильный сертификат, мобильный резервный сертификат ("M", "MR")	Минимальная длина ключа: 2048. Основные ограничения: • CA: Да. • Ограничение длины пути: Отсутствует. Значение ограничения длины пути может быть целым числом, отличным от "None", если общий сертификат имеет значение ограничения длины пути не менее 1. Использование ключа: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (EKU): аутентификация сервера. EKU необязательно, но если оно содержится в вашем сертификате, данные аутентификации сервера должны быть указаны в EKU.
Сертификат, выпущенный доверенным центром сертификации (CA), для автоматически генерируемых пользовательских сертификатов (MCA)	Минимальная длина ключа: 2048. Основные ограничения: • CA: Да. • Ограничение длины пути: Отсутствует. Значение ограничения длины пути может быть целым числом, отличным от "None", если Общий сертификат имеет значение ограничения длины пути не менее 1. Использование ключа: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (англ. Extended Key Usage, EKU): аутентификация клиента. EKU необязателен, но если он содержится в вашем сертификате, данные аутентификации клиента должны быть указаны в EKU.

Сертификаты, выпущенные доверенным центром сертификации (англ. certificate authority, CA), не имеют разрешения на подписывание сертификатов. Чтобы использовать такие сертификаты, убедитесь, что на точках распространения или шлюзах соединения в вашей сети установлен Агент администрирования версии 13 или выше. В противном случае вы не сможете использовать сертификаты без разрешения на подпись.

Этапы

Указание сертификата Сервера администрирования состоит из следующих этапов:

1. **Замена сертификата Сервера администрирования**

   Используйте для этой цели утилиту командной строки klsetsrvcert.

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

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

3. **Указание нового сертификата в параметрах Kaspersky Security Center Web Console**

   После замены сертификата укажите это в параметрах Kaspersky Security Center Web Console. Иначе Kaspersky Security Center Web Console не сможет подключиться к Серверу администрирования.

Результаты

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

Замена сертификата Сервера администрирования с помощью утилиты klsetsrvcert

Чтобы заменить сертификат Сервера администрирования:

В командной строке выполните следующую команду:

```
klsetsrvcert [-t <тип сертификата> {-i <путь к новому сертификату> [-p <пароль>] [-o <параметры>] | -g <dns имя>}][-f <время замены>][-r <корневые сертификаты>][-l <путь к файлу журнала>]
```

Вам не нужно загружать утилиту klsetsrvcert. Утилита входит в состав комплекта поставки Kaspersky Security Center. Она несовместима с предыдущими версиями Kaspersky Security Center.

Описание параметров утилиты klsetsrvcert представлено в таблице ниже.

Значения параметров утилиты klsetsrvcert

Параметр	Значение
`-t <тип сертификата>`	Тип сертификата, который следует заменить. Возможные значения параметра `<тип сертификата>`: • `C` – заменить общий сертификат для портов 13000 и 13291. • `CR` – заменить общий резервный сертификат для портов 13000 и 13291. • `M` – заменить сертификат для мобильных устройств порта 13292. • `MR` – заменить мобильный резервный сертификат для порта 13292. • `MCA` – мобильный сертификат, полученный от доверенного центра сертификации для автоматической генерации пользовательских сертификатов.
`-f <время замены>`	Расписание замены сертификата использует формат "ДД-ММ-ГГГГ ЧЧ:ММ" (для портов 13000 и 13291). Используйте этот параметр, если вы хотите заменить общий сертификат до истечения срока действия общим резервным сертификатом. Укажите время, когда управляемые устройства должны синхронизироваться с Сервером администрирования с использованием нового сертификата.
`-i <путь к новому сертификату>`	Контейнер с сертификатом и закрытый ключ в формате PKCS#12 (файл с расширением p12 или pfx).
`-p <пароль>`	Пароль, при помощи которого защищен p12-контейнер. Сертификат и закрытый ключ хранятся в контейнере, поэтому для расшифровки файла с контейнером требуется пароль.
`-o <параметры проверки>`	Параметры проверки сертификата (разделенные точкой с запятой). Чтобы использовать пользовательский сертификат без разрешения на подпись, в утилите klsetsrvcert укажите `-o NoCA`. Это полезно для сертификатов, выпущенных доверенным центром сертификации (англ. certificate authority, CA). Чтобы изменить длину ключа шифрования для сертификатов типа C или CR, укажите в утилите klsetsrvcert `-o RsaKeyLen:<длина ключа>`, где параметр `<длина ключа>` – это необходимая длина ключа. Иначе используется текущая длина ключа сертификата.
`-g <dns имя>`	Сертификат будет создан с указанным DNS-именем.
`-r <корневые сертификаты>`	Список доверенных корневых сертификатов, подписанных доверенным центром сертификации, в формате PEM.
`-l <путь к файлу журнала>`	Файл вывода результатов. По умолчанию вывод осуществляется в стандартный поток вывода.

Например, для указания пользовательского сертификата Сервера администрирования, используйте следующую команду:

```
klsetsrvcert -t C -i <путь к новому сертификату> -p <пароль> -o NoCA
```

После замены сертификата все Агенты администрирования, подключенные к Серверу администрирования по протоколу SSL, теряют связь. Чтобы восстановить связь, используйте командную строку утилиты klmover.

Чтобы не потерять соединения Агентов администрирования, используйте следующие команды:

1. Чтобы установить новый сертификат,

   ```
   klsetsrvcert.exe -t CR -i <путь к новому сертификату> -p <пароль> -o NoCA
   ```

2. Чтобы указать дату применения нового сертификата,

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

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

Подключение Агентов администрирования к Серверу администрирования с помощью утилиты klmover

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

Чтобы указать новый сертификат Сервера администрирования и восстановить соединение:

В командной строке выполните команду:

```
klmover [-address <адрес сервера>] [-pn <номер порта>] [-ps <номер SSL-порта>] [-nossl] [-cert <путь к файлу сертификата>]
```

Для запуска утилиты требуются права администратора.

Эта утилита автоматически копируется в папку установки Агента администрирования при установке Агента администрирования на клиентское устройство.

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

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

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

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

Описание параметров утилиты klmover представлено в таблице ниже.

Значения параметров утилиты klmover

Параметр	Значение
`-address <адрес сервера>`	Адрес Сервера администрирования для подключения. В качестве адреса можно указать IP-адрес, NetBIOS- или DNS-имя.
`-pn <номер порта>`	Номер порта, по которому будет осуществляться незашифрованное подключение к Серверу администрирования. По умолчанию установлен порт 14000.
`-ps <номер SSL-порта>`	Номер SSL-порта, по которому осуществляется зашифрованное подключение к Серверу администрирования с использованием протокола SSL. По умолчанию установлен порт 13000.

Параметр	Значение
`-nossl`	Использовать незашифрованное подключение к Серверу администрирования. Если ключ не используется, подключение Агента администрирования к Серверу осуществляется по защищенному SSL-протоколу.
`-cert < путь к файлу сертификата >`	Использовать указанный файл сертификата для аутентификации доступа к Серверу администрирования.
`-virtserv`	Имя виртуального Сервера администрирования.
`-cloningmode`	Режим клонирования диска Агента администрирования. Используйте один из следующих параметров для настройки режима клонирования диска: • `-cloningmode` – запрос состояния режима клонирования диска. • `-cloningmode 1` – включить режим клонирования диска. • `-cloningmode 0` – выключить режим клонирования диска.
`-nauninstpwd < пароль >`	Используйте этот параметр, чтобы указать пароль для деинсталляции Агента администрирования. Необязательный параметр.

Например, чтобы подключить Агент администрирования к Серверу администрирования, выполните следующую команду:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

Перевыпуск сертификата Веб-сервера

Сертификат Веб-сервера, используемый в Kaspersky Security Center, необходим для публикации инсталляционных пакетов Агента администрирования, которые вы впоследствии загружаете на управляемые устройства, а также для публикации iOS MDM-профилей, приложений для iOS и инсталляционных пакетов Kaspersky Endpoint Security для мобильных устройств. В зависимости от текущей конфигурации приложения в качестве сертификата Веб-сервера могут использоваться различные сертификаты (подробнее см. О сертификатах Kaspersky Security Center).

Вам может потребоваться перевыпустить сертификат Веб-сервера, чтобы обеспечить соответствие требованиям безопасности вашей организации или для поддержания постоянного соединения ваших управляемых устройств перед началом обновления приложения. Kaspersky Security Center предоставляет два способа перевыпуска сертификата Веб-сервера. Выбор между двумя способами зависит от того, подключены ли у вас мобильные устройства и управляются ли они через мобильный протокол (то есть с помощью мобильного сертификата).

Если вы никогда не указывали пользовательский сертификат в качестве сертификата Веб-сервера в окне **Веб-сервер** свойств Сервера администрирования, мобильный сертификат действует как сертификат Веб-сервера. В этом случае перевыпуск сертификата Веб-сервера выполняется путем перевыпуска самого мобильного протокола.

Чтобы перевыпустить сертификат Веб-сервера, когда у вас нет мобильных устройств, управляемых через мобильный протокол:

1. В дереве консоли, в контекстном меню требуемого Сервера администрирования выберите пункт **Свойства**.
2. В открывшемся окне свойств Сервер администрирования выберите раздел **Параметры подключения к Серверу администрирования**.
3. В списке подразделов выберите подраздел **Сертификаты**.

4. Если вы планируете и дальше использовать сертификат, выданный Kaspersky Security Center:

    a. В группе параметров **Аутентификация Сервера администрирования мобильными устройствами** выберите параметр **Сертификат выпущен средствами Сервера администрирования** и нажмите на кнопку **Перевыпустить**.

    b. В открывшемся окне **Перевыпуск сертификата** в группе параметров **Адрес подключения** и **Срок активации** выберите соответствующие параметры и нажмите на кнопку **ОК**.

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

    Если вы планируете использовать собственный сертификат, выполните следующее:

    a. Проверьте, соответствует ли ваш пользовательский сертификат требованиям Kaspersky Security Center. При необходимости измените сертификат.

    b. Выберите параметр **Другой сертификат** и нажмите на кнопку **Обзор**.

    c. В открывшемся окне **Сертификат** в поле **Тип сертификата** выберите тип вашего сертификата и укажите расположение сертификата и параметры:

    - Если вы выбрали **Контейнер PKCS#12**, нажмите на кнопку **Обзор** рядом с полем **Файл сертификата** и укажите файл сертификата на жестком диске. Если файл сертификата защищен паролем, введите пароль в поле **Пароль (если есть)**.

    - Если вы выбрали **X.509-сертификат**, нажмите на кнопку **Обзор** рядом с полем **Закрытый ключ (.prk, .pem)** и укажите закрытый ключ на жестком диске. Если закрытый ключ защищен паролем, введите пароль в поле **Пароль (если есть)**. Нажмите на кнопку **Обзор** рядом с полем **Открытый ключ (.cer)** и укажите закрытый ключ на жестком диске.

    d. В окне **Сертификат** нажмите на кнопку **ОК**.

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

    Мобильный сертификат перевыпущен для использования в качестве сертификата Веб-сервера.

Чтобы перевыпустить сертификат Веб-сервера, когда у вас есть мобильные устройства, управляемые через мобильный протокол:

1. Создайте пользовательский сертификат и подготовьте его для использования в Kaspersky Security Center. Проверьте, соответствует ли ваш пользовательский сертификат требованиям Kaspersky Security Center. При необходимости измените сертификат.

2. В дереве консоли, в контекстном меню требуемого Сервера администрирования выберите пункт **Свойства**.

3. В открывшемся окне свойств Сервер администрирования выберите раздел **Веб-сервер**.

4. В меню **По протоколу HTTPS** выберите параметр **Задать другой сертификат**.

5. В меню **По протоколу HTTPS** нажмите на кнопку **Изменить**.

6. В открывшемся окне **Сертификат** в поле **Тип сертификата** выберите тип вашего сертификата:

   - Если вы выбрали **Контейнер PKCS#12**, нажмите на кнопку **Обзор** рядом с полем **Файл сертификата** и укажите файл сертификата на жестком диске. Если файл сертификата защищен паролем, введите пароль в поле **Пароль (если есть)**.

   - Если вы выбрали **X.509-сертификат**, нажмите на кнопку **Обзор** рядом с полем **Закрытый ключ (.prk, .pem)** и укажите закрытый ключ на жестком диске. Если закрытый ключ защищен паролем, введите пароль в поле **Пароль (если есть)**. Нажмите на кнопку **Обзор** рядом с полем **Открытый ключ (.cer)** и укажите закрытый ключ на жестком диске.

7. В окне **Сертификат** нажмите на кнопку **ОК**.

8. При необходимости в окне свойств Сервера администрирования в поле **HTTPS-порт Веб-сервера** измените номер HTTPS-порта для Веб-сервера. Нажмите на кнопку **ОК**.

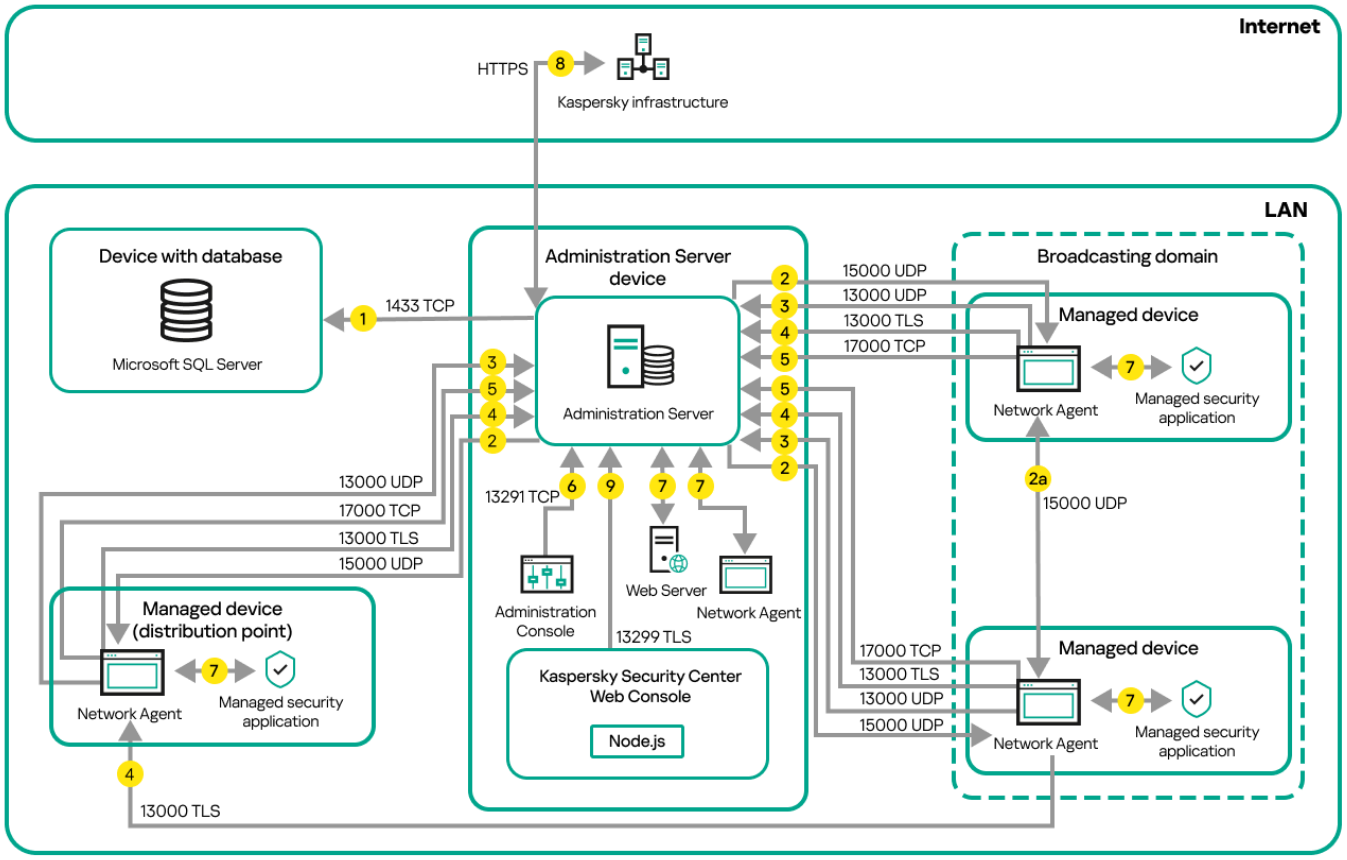
   Сертификат Веб-сервера перевыпущен.

Схемы трафика данных и использования портов

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

Сервер администрирования и управляемые устройства в локальной сети (LAN)

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



Сервер администрирования и управляемые устройства в локальной сети (LAN)

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

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

1. Сервер администрирования передает данные в базу данных. Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server или порт 1433 для Microsoft SQL Server). Подробную информацию см. в документации СУБД.

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

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

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

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

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

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

   > Точка распространения в ранних версиях Kaspersky Security Center называлась агентом обновлений.

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

6. Данные от Консоли администрирования на основе консоли Microsoft Management Console передаются на Сервер администрирования через порт 13291. Консоль администрирования может быть установлена на том же устройстве или на другом.

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

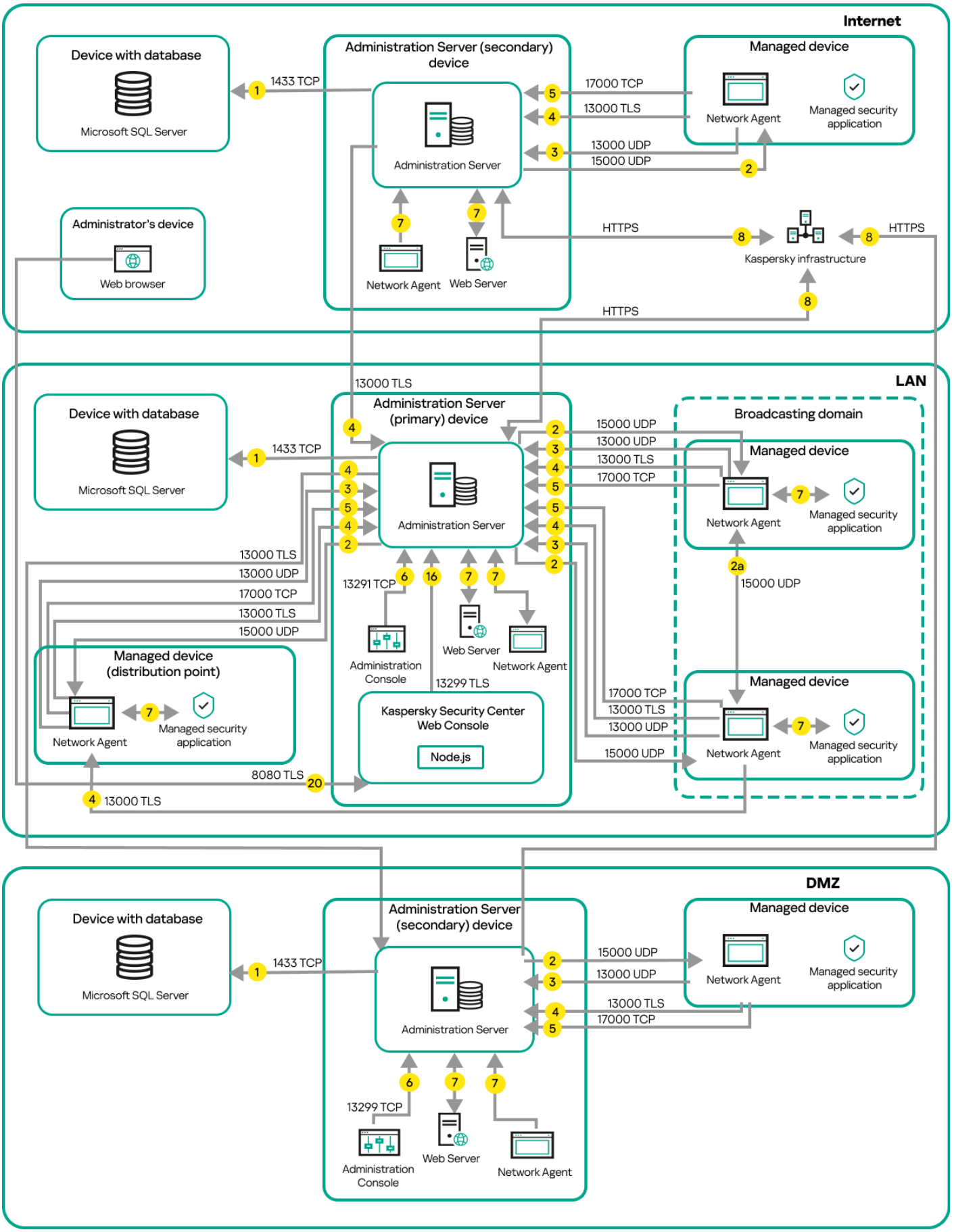
8. Данные от Сервера администрирования к серверам "Лаборатории Касперского" (например, данные KSN, информация о лицензиях) и данные от серверов "Лаборатории Касперского" к Серверу администрирования (например, обновления приложений и обновления антивирусных баз) передаются по протоколу HTTPS.

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

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

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

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



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

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

1. Сервер администрирования передает данные в базу данных. Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server или порт 1433 для Microsoft SQL Server). Подробную информацию см. в документации СУБД.

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

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

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

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

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

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

   > Точка распространения в ранних версиях Kaspersky Security Center называлась агентом обновлений.

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

6. Данные от Консоли администрирования на основе консоли Microsoft Management Console передаются на Сервер администрирования через порт 13291. Консоль администрирования может быть установлена на том же устройстве или на другом.

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

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

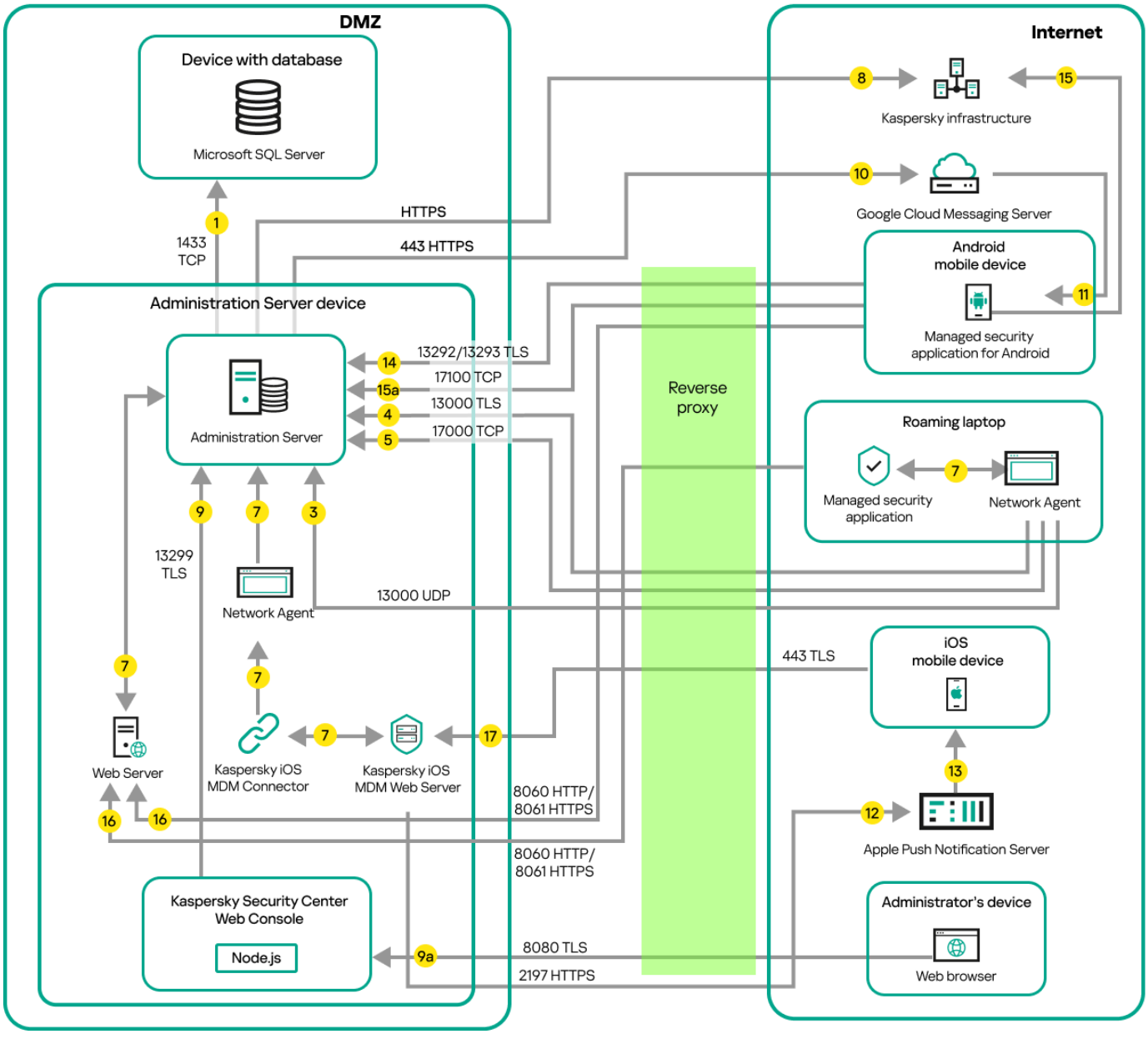
   Если вы не хотите иметь доступ в интернет на вашем Сервере администрирования, вам нужно управлять этими данными вручную.

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

   9a. Данные от браузера, установленного на отдельном устройстве администратора, передаются на Сервер Kaspersky Security Center Web Console через TLS-порт 8080. Сервер Kaspersky Security Center Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.

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

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



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

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

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

1. Сервер администрирования передает данные в базу данных. Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server или порт 1433 для Microsoft SQL Server). Подробную информацию см. в документации СУБД.

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

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

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

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

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

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

   > Точка распространения в ранних версиях Kaspersky Security Center называлась агентом обновлений.

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

6. Данные от Консоли администрирования на основе консоли Microsoft Management Console передаются на Сервер администрирования через порт 13291. Консоль администрирования может быть установлена на том же устройстве или на другом.

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

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

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

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

   9a. Данные от браузера, установленного на отдельном устройстве администратора, передаются на Сервер Kaspersky Security Center Web Console через TLS-порт 8080. Сервер Kaspersky Security Center Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.

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

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

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

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

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

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

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

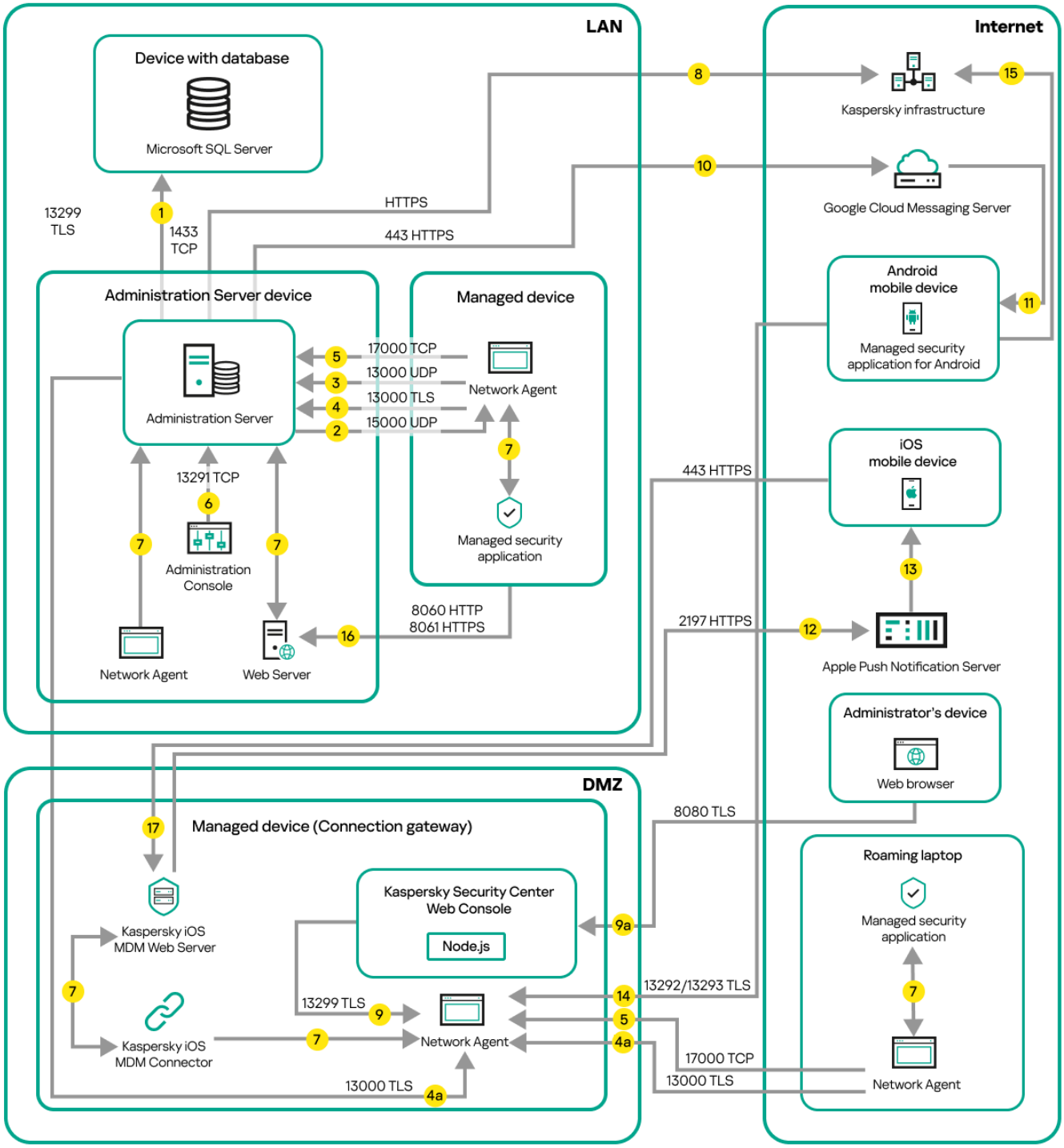
16. Запросы на пакеты от управляемых устройств, включая мобильные устройства, передаются на Веб-сервер, который находится на том же устройстве, на котором установлен Сервер администрирования.

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

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

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

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



Управляемые мобильные устройства, подключенные к Серверу администрирования через шлюз соединения

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

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

1. Сервер администрирования передает данные в базу данных. Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server или порт 1433 для Microsoft SQL Server). Подробную информацию см. в документации СУБД.

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

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

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

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

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

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

   > Точка распространения в ранних версиях Kaspersky Security Center называлась агентом обновлений.

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

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

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

6. Данные от Консоли администрирования на основе консоли Microsoft Management Console передаются на Сервер администрирования через порт 13291. Консоль администрирования может быть установлена на том же устройстве или на другом.

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

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

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

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

   9a. Данные от браузера, установленного на отдельном устройстве администратора, передаются на Сервер Kaspersky Security Center Web Console через TLS-порт 8080. Сервер Kaspersky Security Center Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.

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

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

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

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

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

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

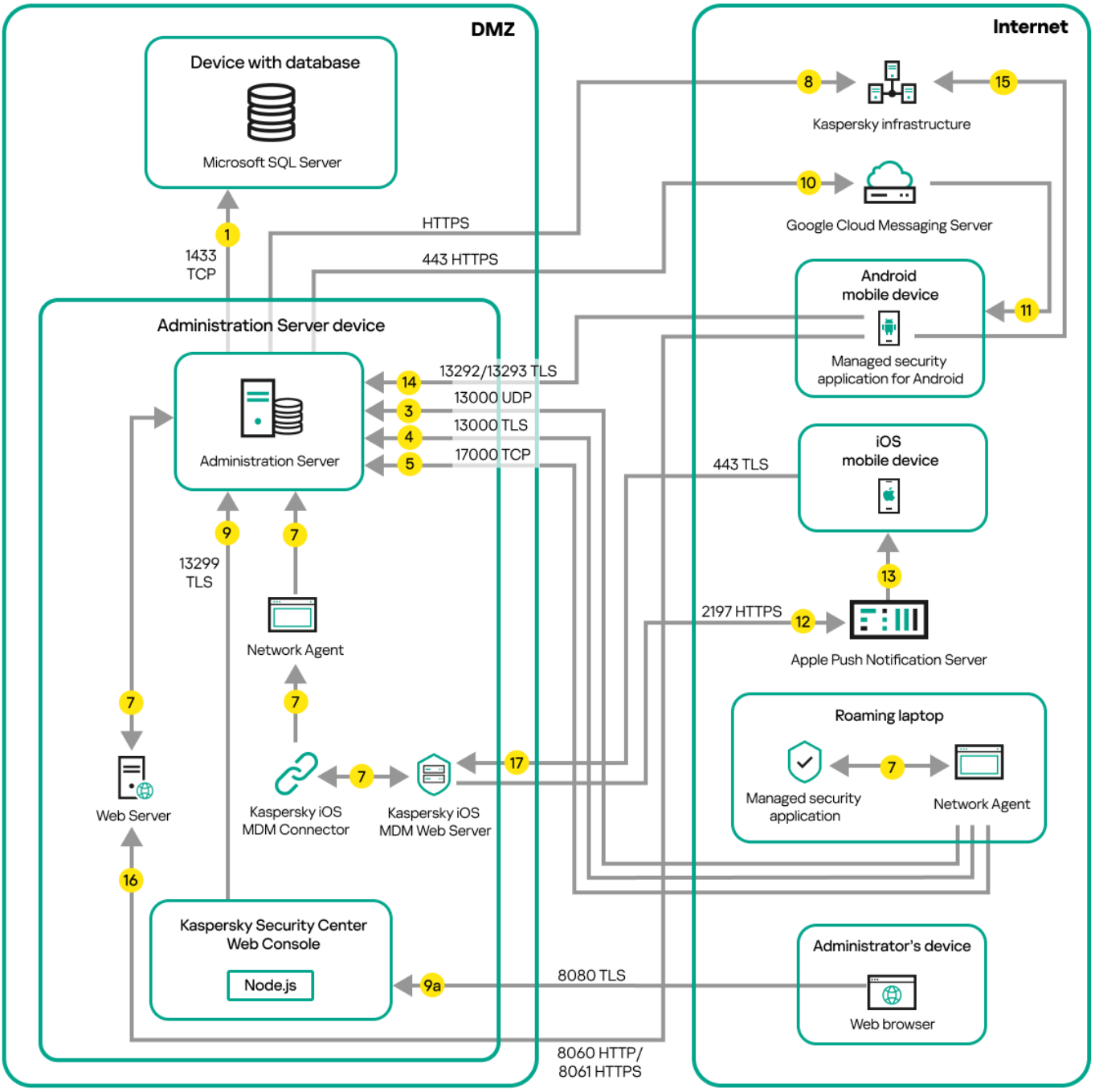
    Если мобильное устройство не имеет доступа в интернет, данные передаются на Сервер администрирования через порт 17100, а Сервер администрирования передает их инфраструктуре "Лаборатории Касперского". Однако этот сценарий используется очень редко.

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

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

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

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



Сервер администрирования в демилитаризованной зоне, управляемые мобильные устройства в интернете

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

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

1. Сервер администрирования передает данные в базу данных. Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server или порт 1433 для Microsoft SQL Server). Подробную информацию см. в документации СУБД.

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

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

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

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

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

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

   > Точка распространения в ранних версиях Kaspersky Security Center называлась агентом обновлений.

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

6. Данные от Консоли администрирования на основе консоли Microsoft Management Console передаются на Сервер администрирования через порт 13291. Консоль администрирования может быть установлена на том же устройстве или на другом.

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

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

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

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

   9a. Данные от браузера, установленного на отдельном устройстве администратора, передаются на Сервер Kaspersky Security Center Web Console через TLS-порт 8080. Сервер Kaspersky Security Center Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.

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

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

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

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

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

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

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

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

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

Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения

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

Условные обозначения в схемах взаимодействия

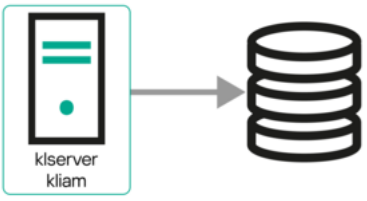
В таблице ниже приведены условные обозначения, использованные в схемах.

Условные обозначения

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

Сервер администрирования и СУБД

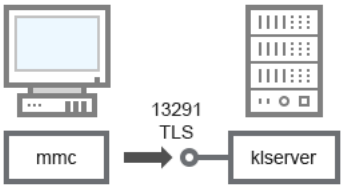
Данные от Сервера администрирования поступают в базу данных SQL Server, MySQL или MariaDB.



Сервер администрирования и СУБД

Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server или порт 1433 для Microsoft SQL Server). Подробную информацию см. в документации СУБД.

Сервер администрирования и Консоль администрирования



Сервер администрирования и Консоль администрирования

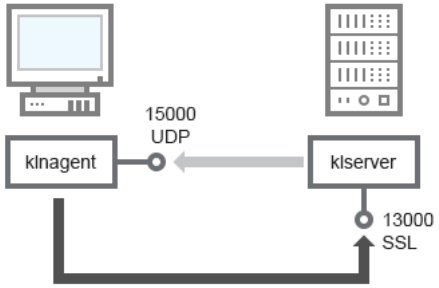
Пояснения к схеме см. в таблице ниже.

Сервер администрирования и Консоль администрирования (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта
Сервер администрирования	13291	klserver	TCP	Да	Прием подключений от Консоли администрирования

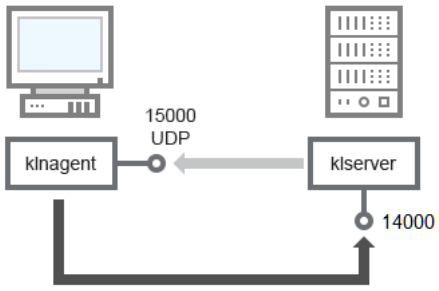
Сервер администрирования и клиентское устройство: Управление приложением безопасности

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



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

Если вы использовали Kaspersky Security Center одной из предыдущих версий, то в вашей сети Сервер администрирования может принимать подключения от Агентов администрирования по незащищенному порту 14000 (см. рис. ниже). Kaspersky Security Center 15.1 также поддерживает подключение Агентов администрирования по порту 14000, однако рекомендуется использовать защищенный порт 13000.



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

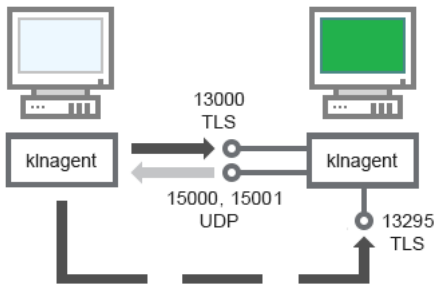
Пояснения к схемам см. в таблице ниже.

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

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

Обновление программного обеспечения на клиентском устройстве с помощью точки распространения

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



Обновление программного обеспечения на клиентском устройстве с помощью точки распространения

Пояснения к схеме см. в таблице ниже.

Обновление программного обеспечения с помощью точки распространения (трафик)

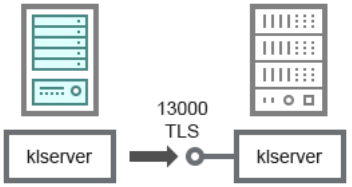
Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS (только для TCP)	Назначение порта
Агент администрирования	15000	klnagent	UDP	Нет значения	Многоадресная рассылка Агентам администрирования
Агент администрирования	15001	klnagent	UDP	Нет значения	Получение обновлений и инсталляционных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

Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования

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

При объединении Серверов в иерархию необходимо, чтобы порт 13291 обоих Серверов был доступен. Через порт 13291 происходит подключение Консоли администрирования к Серверу администрирования.

В дальнейшем, после объединения Серверов в иерархию, вы сможете администрировать оба Сервера через Консоль администрирования, подключенную к главному Серверу администрирования. Таким образом, необходимо только, чтобы порт 13291 главного Сервера был доступен.



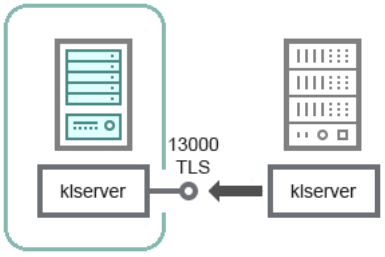
Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования

Пояснения к схеме см. в таблице ниже.

Иерархия Серверов администрирования (трафик)

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

Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне



Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне

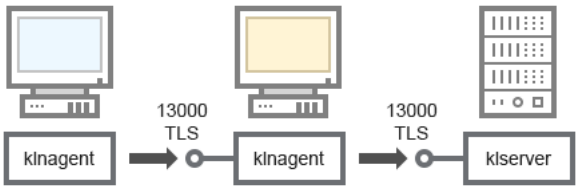
На схеме показана иерархия Серверов администрирования, в которой подчиненный Сервер, находящийся в демилитаризованной зоне, принимает подключение от главного Сервера (пояснения к схеме см. в таблице ниже). При объединении Серверов в иерархию необходимо, чтобы порт 13291 обоих Серверов был доступен. Через порт 13291 происходит подключение Консоли администрирования к Серверу администрирования.

В дальнейшем, после объединения Серверов в иерархию, вы сможете администрировать оба Сервера через Консоль администрирования, подключенную к главному Серверу администрирования. Таким образом, необходимо только, чтобы порт 13291 главного Сервера был доступен.

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

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

Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство



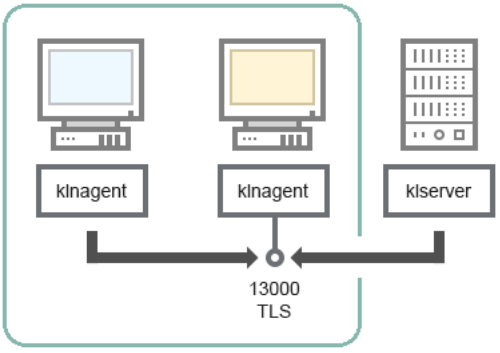
Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство

Пояснения к схеме см. в таблице ниже.

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

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

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



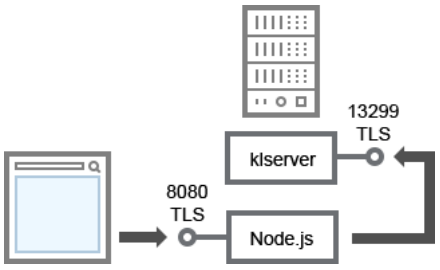
Сервер администрирования, шлюз соединений и клиентское устройство в демилитаризованной зоне

Пояснения к схеме см. в таблице ниже.

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

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

Сервер администрирования и Kaspersky Security Center Web Console



Сервер администрирования и Kaspersky Security Center Web Console

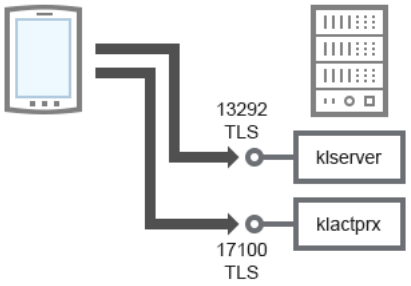
Пояснения к схеме см. в таблице ниже.

Сервер администрирования и Kaspersky Security Center Web Console (трафик)

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

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

Активация и управление приложением безопасности на мобильном устройстве



Активация и управление приложением безопасности на мобильном устройстве

Пояснения к схеме см. в таблице ниже.

Активация и управление приложением безопасности на мобильном устройстве (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта
Сервер администрирования	13292	klserver	TCP	Да	Прием подключений от Консоли администрирования к Серверу администрирования
Сервер администрирования	17100	klactprx	TCP	Да	Прием подключений для активации приложений от мобильных устройств

Лучшие практики развертывания

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

- Сервер администрирования – центральный компонент, ответственный за управление устройствами организации и хранение данных в СУБД.
- Консоль администрирования – основной инструмент администратора. Консоль администрирования поставляется вместе с Сервером администрирования, но может быть также установлена отдельно на одно или несколько устройств администратора.
- Агент администрирования – служит для управления установленным на устройстве приложением безопасности, а также для получения информации об устройстве и передаче этой информации на Сервер администрирования. Агенты администрирования устанавливаются на устройства организации.

Развертывание Kaspersky Security Center в сети организации осуществляется следующим образом:

- установка Сервера администрирования;
- установка Консоли администрирования на устройстве администратора;
- установка Агента администрирования и приложения безопасности на устройства организации.

Руководство по усилению защиты

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

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

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

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

Руководство по усилению защиты содержит следующую информацию:

- выбор схемы развертывания Сервера Администрирования;
- настройка безопасного подключения к Серверу Администрирования;

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

Развертывание Сервера администрирования

Архитектура Сервера администрирования

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

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

На основании этой информации нужно сформировать архитектуру, определяющую:

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

Выбор устройства для Сервера администрирования

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

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

Расположение Сервера администрирования

Устройства, управляемые Сервером администрирования, могут располагаться:

- в локальном сегменте сети;
- в интернете;
- в демилитаризованной зоне (DMZ).

При этом Сервер администрирования также может быть расположен в следующих сегментах: технологическом, корпоративном, сегментах демилитаризованной зоны (DMZ).

При использовании Kaspersky Security Center для управления защитой изолированного сегмента сети, рекомендуется разворачивать Сервер администрирования в сегменте демилитаризованной зоны (DMZ). Это позволит организовать полноценное сегментирование сетей и минимизировать возможные обращения в защищаемый сегмент, сохранив при этом возможности по управлению устройствами и доставке обновлений.

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

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

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

Например, ограничения безопасности, применяемые к контроллеру домена, могут значительно снизить производительность Сервера администрирования и привести к невозможности использования некоторых его функций. Если привилегированный доступ к контроллеру домена получит злоумышленник, он может изменить, повредить или уничтожить базу данных Active Directory Domain Services (AD DS). При этом также будут скомпрометированы все системы и учетные записи, управляемые Active Directory.

Учетные записи для установки и запуска Сервера администрирования

Рекомендуется запустить установку Сервера администрирования под учетной записью локального администратора, чтобы избежать использования учетных записей домена для доступа к базе данных Сервера администрирования. Набор необходимых учетных записей и их прав зависит от выбранного типа СУБД, местоположения СУБД и способа создания базы данных Сервера администрирования.

Группы пользователей KLAdmins и KLOperators создаются автоматически во время установки Kaspersky Security Center. Этим группам предоставляются права на подключение к Серверу администрирования и на работу с его объектами.

В зависимости от того, под какой учетной записью проводится установка Kaspersky Security Center, группы KLAdmins и KLOperators создаются следующим образом:

- Если установка проводится под учетной записью пользователя, входящего в домен, группы создаются на устройстве с Сервером администрирования и в домене, в который входит устройство с Сервером администрирования.
- Если установка проводится под учетной записью системы, группы создаются только на устройстве с Сервером администрирования.

Чтобы избежать создания групп KLAdmins и KLOperators в домене и, как следствие, **присвоения прав для управления Сервером администрирования вне устройства, на котором он установлен**, рекомендуется проводить установку Kaspersky Security Center под локальной учетной записью.

При установке Сервера администрирования выберите учетную запись, под которой Сервер администрирования будет запускаться как служба. По умолчанию приложение создает локальную учетную запись KL-AK-*, под которой будет запускаться служба Сервера администрирования (klserver).

Служба Сервера администрирования при необходимости может запускаться под выбранной учетной записью. При этом учетная запись должна обладать различными правами для подключения к СУБД. Для обеспечения безопасности используйте непривилегированную учетную запись для запуска службы Сервера администрирования.

Во избежание некорректных параметров доступа для учетной записи Сервера администрирования рекомендуется создавать ее автоматически.

Исключение Сервера администрирования из домена

Если вы используете Сервер администрирования для защиты групп устройств важных систем, не рекомендуется включать в домен устройство Сервера администрирования. Это позволит разграничить права управления Kaspersky Security Center и избежать получения доступа к управлению в случае компрометации домена.

Обратите внимание, если вы установите Сервер администрирования на устройство, входящее в рабочую группу, будут недоступны следующие сценарии работы с Сервером администрирования:

- Использование отказоустойчивого кластера Kaspersky Security Center.
- Использование отказоустойчивого кластера Windows Server.
- Использование SQL Server для Windows на отдельном устройстве.

  Использовать SQL Server для Windows на отдельном устройстве можно, только если Сервер администрирования и SQL Server находятся в одном домене или на доверенных доменах. Если Сервер администрирования, SQL Server и общая папка UNC для резервных копий находятся в рабочей группе, вы не можете безопасно настроить права доступа Чтение и Запись между SQL Server и общей папкой.
- Удаленная установка средствами Сервера администрирования с помощью групповых политик Active Directory

Если вам нужно отключить Сервер администрирования от домена Active Directory, следуйте шагам, описанным в разделе Как изменить имя Сервера администрирования Kaspersky Security Center.

Если необходимо установить Сервер администрирования на устройство, входящее в рабочую группу, также можно использовать Kaspersky Security Center Linux вместо Kaspersky Security Center Windows.

Безопасность соединения

Использование TLS

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

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

Строгие параметры TLS

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

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

Запрет удаленной аутентификации с учетными записями Windows

Запрет на SSPI-подключения с удаленных адресов возможен с помощью специального флага LP_RestrictRemoteOsAuth. Этот флаг позволяет запретить удаленную аутентификацию на Сервере администрирования для учетных записей Windows, локальных или доменных.

Чтобы переключить флаг LP_RestrictRemoteOsAuth в режим запрета SSPI-подключений с удаленных адресов:

1. Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Выполните следующую команду в командной строке, чтобы указать значение флага LP_RestrictRemoteOsAuth:

   ```
   klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_RestrictRemoteOsAuth -t d -v 1
   ```

3. Перезапустите службу Сервера администрирования.

Флаг LP_RestrictRemoteOsAuth не работает, если удаленная аутентификация выполняется через Kaspersky Security Center Web Console или Консоль администрирования, установленную на том же устройстве, что и Сервер администрирования.

Ограничение доступа к базе данных Сервера администрирования

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

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

Аутентификация Microsoft SQL Server

Если Kaspersky Security Center использует Microsoft SQL Server в качестве СУБД, необходимо защитить от несанкционированного доступа данные Kaspersky Security Center, передаваемые в базу данных или получаемые из нее, а также данные, хранящиеся в базе данных. Для этого требуется настроить использование безопасного соединения между Kaspersky Security Center и SQL Server. Самый надежный способ обеспечить безопасную связь – это установить Kaspersky Security Center и SQL Server на одном устройстве и использовать механизм совместной памяти для обоих приложений. Во всех других случаях рекомендуется использовать сертификат SSL/TLS для аутентификации экземпляра SQL Server.

Сервер администрирования может обращаться к SQL Server с помощью следующих провайдеров:

- SQLOLEDB с помощью TCP/IP или Named Pipes.

  Этот провайдер установлен в операционной системе Windows и используется по умолчанию.

- MSOLEDBSQL с помощью TCP/IP, Named Pipes или Shared memory.

  Если вы хотите использовать этот провайдер, вам нужно установить его на устройстве с Сервером администрирования, а затем установить значение `1` в глобальную переменную среды `KLDBADO_UseMSOLEDBSQL`.

- MSOLEDBSQL19 с помощью TCP/IP, Named Pipes или Shared memory.

  Если вы хотите использовать этот провайдер, вам нужно установить его на устройство с Сервером администрирования, а затем установить значение `1` в глобальную переменную среды `KLDBADO_UseMSOLEDBSQL` и значение `MSOLEDBSQL19` в глобальную переменную среды `KLDBADO_ProviderName`.

Также прежде чем использовать TCP/IP, Named Pipes или Shared memory, убедитесь, что включен необходимый протокол.

Безопасность взаимодействия с внешней СУБД

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

Настройка списка разрешенных IP-адресов для подключения к Серверу администрирования

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

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

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

Безопасное подключение к контроллеру домена во время опроса

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

Учетные записи и авторизация

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

Использование двухфакторной аутентификации Сервера администрирования

Kaspersky Security Center предоставляет пользователям Kaspersky Security Center Web Console и Консоли администрирования возможность использовать **двухфакторную аутентификацию** на основе стандарта RFC 6238 (TOTP: Time-Based One-Time Password algorithm).

Если для вашей учетной записи включена двухфакторная аутентификация, каждый раз при входе в Kaspersky Security Center Web Console или в Консоль администрирования вы вводите свое имя пользователя, пароль и дополнительный одноразовый код безопасности. Если вы используете доменную аутентификацию для своей учетной записи, вам необходимо ввести только дополнительный одноразовый код безопасности. Для того чтобы получить одноразовый код безопасности, вам нужно установить приложение для аутентификации на своем компьютере или мобильном устройстве.

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

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

Запрет новым пользователям настраивать для себя двухфакторную аутентификацию

Чтобы еще больше повысить безопасность доступа к Kaspersky Security Center Web Console, вы можете запретить новым пользователям настраивать для себя двухфакторную аутентификацию.

Если этот параметр включен, пользователь с выключенной двухфакторной аутентификацией, например новый администратор домена, не сможет настроить двухфакторную аутентификацию для себя. Следовательно, такой пользователь не может быть аутентифицирован на Сервере администрирования и не может войти в Kaspersky Security Center Web Console без одобрения другого администратора Kaspersky Security Center, у которого уже включена двухфакторная аутентификация.

Использование двухфакторной аутентификации операционной системы

Для авторизации на устройстве с Сервером администрирования рекомендуется использовать многофакторную аутентификацию (MFA) с использованием токена, смарт-карты или другого способа.

Запрет на сохранение пароля администратора

При использовании Консоли администрирования не рекомендуется сохранять пароль администратора в диалоговом окне подключения к Серверу администрирования.

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

Авторизация внутреннего пользователя

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

- Длина пароля должна быть от 8 до 256 символов.
- Пароль должен содержать символы как минимум трех групп из списка ниже:
  - верхний регистр (A–Z);
  - нижний регистр (a–z);
  - числа (0–9);
  - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
- Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", когда "." расположена перед "@".

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

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

Настройка параметров смены пароля внутренней учетной записи пользователя

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

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

Защита учетной записи от несанкционированного изменения

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

Отдельная группа администрирования для устройства с Сервером администрирования

Для Сервера администрирования

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

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

Группы KLAdmins и KLOperators

Группы пользователей KLAdmins и KLOperators создаются автоматически во время установки Kaspersky Security Center. Группе KLAdmins предоставлены все права. Группе KLOperators предоставлены права на Чтение и Выполнение. Набор прав, предоставленных группе KLAdmins, **недоступен для изменения**.

С помощью стандартных средств администрирования операционной системы можно просмотреть группы KLAdmins и KLOperators и внести изменения в состав этих групп.

При разработке регламентов работы с Сервером администрирования нужно определить, потребуется ли специалисту информационной безопасности полный доступ (и включение в группу KLAdmins) для решения штатных задач.

Большинство базовых задач администрирования могут быть распределены между подразделениями организации (или разными сотрудниками одного подразделения) и, как следствие, между различными учетными записями. Также может быть выполнено разграничение по доступу к группам администрирования в Kaspersky Security Center. В результате можно реализовать такую модель использования, при которой авторизация под учетными записями из группы KLAdmins будет нестандартным поведением, что можно рассматривать как инцидент.

Если установка Kaspersky Security Center проводилась под системной учетной записью, группы создаются только на устройстве с Сервером администрирования. В этом случае рекомендуем убедиться, что в группу включены только учетные записи, созданные во время установки Kaspersky Security Center. Не рекомендуется добавлять в группу KLAdmins другие группы пользователей (локальные и/или доменные), которые были созданы автоматически во время установки Kaspersky Security Center. Также следует ограничить права на изменение этой группы. Группа KLAdmins должна включать единичные непривилегированные учетные записи.

Если установка выполнялась под учетной записью пользователя, входящего в домен, группы KLAdmins и KLOperators создаются как на Сервере администрирования, так и в домене, в который входит Сервер администрирования. Рекомендуется применить аналогичный подход как и в случае с установкой под системной учетной записью.

Ограничить членство в роли "Главный администратор"

Рекомендуется ограничить членство пользователей в роли "Главный администратор".

По умолчанию после установки Сервера администрирования роль "Главный администратор" присвоена группе локальных администраторов устройства и созданной группе KLAdmins. 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.

Локальных администраторов можно исключить из списка пользователей, имеющих права администратора Kaspersky Security Center. Роль "Главный администратор" нельзя удалить из группы KLAdmins. В нее можно включить учетные записи группы KLAdmins, которые будут использоваться для управления Сервером администрирования.

В случае использования доменной аутентификации, рекомендуется ограничить привилегии учетных записей администраторов домена в Kaspersky Security Center. По умолчанию этим учетным записям присвоена роль "Главный администратор". Также администратор домена может включить свою учетную запись в группу KLAdmins с целью получения роли "Главный администратор". Чтобы этого избежать, в параметрах безопасности Kaspersky Security Center можно добавить группу "Администраторы домена" ("Domain Admins") и определить для нее запрещающие правила. Эти правила будут приоритетнее разрешающих.

Также можно использовать предопределенные роли пользователей с уже 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.

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

Основные преимущества ролевой модели управления доступом:

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

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

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

- Управление группами администрирования.
- Операции с Сервером администрирования.
- Удаленная установка.
- Изменение параметров хранения событий и отправки уведомлений.

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

Отдельная учетная запись для удаленной установки приложений

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

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

Обеспечение безопасности привилегированного доступа Windows

Рекомендуется рассмотреть рекомендации Microsoft по обеспечению безопасности привилегированного доступа. Чтобы просмотреть эти рекомендации, перейдите в раздел Обеспечение безопасности привилегированного доступа.

Одной из ключевых рекомендаций является развертывание рабочих станций с привилегированным доступом (PAW).

Использование управляемых учетных записей служб (MSA) и групповых управляемых учетных записей служб (gMSA) для запуска служб Сервера администрирования

В Active Directory существует специальный тип учетных записей для безопасного запуска служб – MSA/gMSA. Kaspersky Security Center поддерживает управляемые учетные записи службы (MSA) и групповые управляемые учетные записи службы (gMSA). Если такие учетные записи используются в вашем домене, вы можете выбрать одну из них в качестве учетной записи для службы Сервера администрирования.

Регулярный аудит всех пользователей и их действий

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

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

Управление защитой Сервера администрирования

Выбор приложения защиты Сервера администрирования

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

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

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

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

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

Создание отдельной политики безопасности для защиты приложения

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

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

Модули защиты

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

Настройка сетевого экрана устройства с Сервером администрирования

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

По умолчанию Сервер администрирования использует порт 13291 для подключения к Консоли администрирования и порт 13299 для подключения к Kaspersky Security Center Web Console. Рекомендуется ограничить число устройств, с которых Сервер администрирования может управляться по этим портам.

Управление защитой Агента администрирования

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

Использование пароля деинсталляции

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

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

Использование усиленной защиты Агента администрирования

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

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

Отслеживание адреса Сервера администрирования, к которому подключается Агент администрирования

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

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

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

Событие с адресом Сервера администрирования регистрируется в следующих случаях:

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

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

Чтобы настроить выгрузку событий из Kaspersky Event Log:

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

Управление защитой клиентских устройств

Ограничение добавления лицензионных ключей в инсталляционные пакеты

Инсталляционные пакеты хранятся в папке общего доступа Сервера администрирования, во вложенной папке Packages. Если лицензионные ключи будут добавлены в инсталляционный пакет, они могут быть доступны на чтение всем пользователям, имеющим права на чтение этой папки общего доступа.

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

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

Правила автоматического перемещения устройств между группами администрирования

Рекомендуется ограничить использование правил автоматического перемещения устройств между группами администрирования.

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

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

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

Требования безопасности к устройствам с точками распространения и шлюзам соединений

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

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

Размещение точек распространения в сети организации используется для следующих задач:

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

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

Ограничение автоматического назначения точек распространения

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

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

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

Требования безопасности к устройствам пользователей Kaspersky Security Center

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

К устройствам пользователей Kaspersky Security Center относятся следующие устройства:

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

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

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

Настройка защиты управляемых приложений

Политики управляемых приложений

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

Установка пароля на выключение защиты и удаление приложения

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, Kaspersky Security для Windows Servers, Агента администрирования и других приложений "Лаборатории Касперского". После включения защиты паролем рекомендуется заблокировать эти параметры, закрыв их "замком".

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

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

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

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

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

Использование Kaspersky Security Network

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

Регулярная проверка управляемых устройств

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

Обнаружение новых устройств

Рекомендуется должным образом настроить параметры обнаружения устройств: настроить интеграцию с 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.

Определение папки общего доступа

Если Сервер администрирования развернут на устройстве под управлением Windows, при выборе существующей папки общего доступа, (которая используется, например, для размещения инсталляционных пакетов и хранилища обновляемых баз) рекомендуем убедиться, что права на чтение предоставлены группе "Все" (Everyone), а права на запись – группе KLAdmins.

Обслуживание Сервера администрирования

Резервное копирование данных Сервера администрирования

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

По умолчанию задача резервного копирования создается автоматически после установки Сервера администрирования и выполняется периодически с сохранением резервных копий в соответствующей директории.

Пользователь может изменить параметры задачи резервного копирования:

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

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

Обслуживание Сервера администрирования

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

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

- проверяет базу данных на наличие ошибок;
- перестраивает индексы базы данных;
- обновляет статистику базы данных;
- сжимает базу данных (при необходимости).

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

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

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

Передача событий в сторонние системы

Мониторинг и отчеты

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

Экспорт событий в SIEM-системы

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

Уведомление по электронной почте о событиях аудита

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

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

Статистическая информация о работе Сервера администрирования

Для своевременного реагирования на проблемы безопасности рекомендуется настроить отправку статистической информации работы Сервера администрирования приложениям сторонних производителей с помощью протокола Simple Network Management Protocol (SNMP).

Рекомендации по безопасности сторонних информационных систем

Рекомендации по безопасности CIS Benchmarks

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

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

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

- Операционные системы следующих семейств:
  - Windows для рабочих станций
  - Windows для серверов

    - Debian
    - Ubuntu
    - CentOS
    - Oracle Linux
    - Red Hat Enterprise Linux
    - SUSE Linux Enterprise Server
    - macOS
- Платформы виртуализации VMware
- Серверы баз данных:
    - Microsoft SQL Server
    - MySQL
    - MariaDB
    - PostgreSQL

Рекомендации по безопасности для операционной системы Astra Linux

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

Рекомендации по безопасности для операционной системы РЕД ОС

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

Рекомендации по использованию приложений безопасности "Лаборатории Касперского"

Использование пароля KLAdmin в Kaspersky Endpoint Security для Windows

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.

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

- **Общие требования.**

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

- **Требования к минимальной длине пароля.**

  Создайте пароль, который содержит не менее 10 символов.

- **Требования использования нескольких типов символов.**

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

- **Требования к сроку действия пароля.**

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

Подготовка к развертыванию

В этом разделе описаны шаги, которые вам нужно выполнить перед развертыванием Kaspersky Security Center.

Планирование развертывания Kaspersky Security Center

Этот раздел содержит информацию об оптимальных вариантах развертывания компонентов Kaspersky Security Center в сети организации в зависимости от следующих критериев:

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

Типовые способы развертывания системы защиты

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

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

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

- Развертывание системы защиты средствами Kaspersky Security Center одним из следующих способов:
  - через Консоль администрирования;
  - через Kaspersky Security Center Web Console.

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

  Основной схемой развертывания является развертывание системы защиты через Консоль администрирования. Использование Kaspersky Security Center Web Console позволяет запускать установку приложений "Лаборатории Касперского" через браузер.
- Развертывание системы защиты вручную с помощью автономных инсталляционных пакетов, сформированных в Kaspersky Security Center.

  Установка приложений "Лаборатории Касперского" на клиентские устройства и рабочее место администратора производится вручную, параметры подключения клиентских устройств к Серверу администрирования задаются при установке Агента администрирования.

  Этот вариант развертывания рекомендуется применять в случаях, когда невозможно провести удаленную установку.

Kaspersky Security Center также позволяет разворачивать систему защиты с помощью групповых политик Microsoft Active Directory®.

О планировании развертывания Kaspersky Security Center в сети организации

Один Сервер администрирования может обслуживать не более чем 100 000 устройств. Если общее количество устройств в сети организации превышает 100 000, следует разместить в сети организации несколько Серверов администрирования, объединенных в иерархию для удобства централизованного управления.

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

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

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

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

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

Выбор структуры защиты организации

Выбор структуры защиты организации определяют следующие факторы:

- Топология сети организации.
- Организационная структура.
- Число сотрудников, отвечающих за защиту сети, и распределение обязанностей между ними.
- Аппаратные ресурсы, которые могут быть выделены для установки компонентов управления защитой.

- Пропускная способность каналов связи, которые могут быть выделены для работы компонентов защиты в сети организации.

- Допустимое время выполнения важных административных операций в сети организации. К важным административным операциям относятся, например, распространение обновлений антивирусных баз и изменение политик для клиентских устройств.

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

Для анализа сетевой и аппаратной инфраструктуры рекомендуется следующий порядок действий:

1. Определить следующие параметры сети, в которой будет развертываться защита:

   - число сегментов сети;

   - скорость каналов связи между отдельными сегментами сети;

   - число управляемых устройств в каждом из сегментов сети;

   - пропускную способность каждого канала связи, которая может быть выделена для работы защиты.

2. Определить допустимое время выполнения ключевых операций администрирования для всех управляемых устройств.

3. Проанализировать информацию из пунктов 1 и 2, а также данные нагрузочного тестирования системы администрирования. На основании проведенного анализа ответить на следующие вопросы:

   - Возможно ли обслуживание всех клиентов одним Сервером администрирования или требуется иерархия Серверов администрирования?

   - Какая аппаратная конфигурация Серверов администрирования требуется для обслуживания всех клиентов за время, определенное в пункте 2?

   - Требуется ли использование точек распространения для снижения нагрузки на каналы связи?

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

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

- Один Сервер администрирования. Все клиентские устройства подключены к одному Серверу администрирования. Роль точки распространения выполняет Сервер администрирования.

- Один Сервер администрирования с точками распространения. Все клиентские устройства подключены к одному Серверу администрирования. В сети выделены клиентские устройства, выполняющие роль точек распространения.

- Иерархия Серверов администрирования. Для каждого сегмента сети выделен отдельный Сервер администрирования, включенный в общую иерархию Серверов администрирования. Роль точки распространения выполняет главный Сервер администрирования.

- Иерархия Серверов администрирования с точками распространения. Для каждого сегмента сети выделен отдельный Сервер администрирования, включенный в общую иерархию Серверов администрирования. В сети выделены клиентские устройства, выполняющие роль точек распространения.

Типовые конфигурации Kaspersky Security Center

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

- один офис;
- несколько крупных географически распределенных офисов с собственными администраторами;
- множество небольших географически распределенных офисов.

Типовая конфигурация: один офис

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

Один Сервер администрирования может обслуживать до 100 000 устройств. Вам нужно учесть возможность увеличения количества управляемых устройств в ближайшем будущем: может оказаться желательным подключение несколько меньшего количества устройств к одному Серверу администрирования.

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

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

Типовая конфигурация: несколько крупных офисов с собственными администраторами

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

При наличии сотрудников, которые перемещаются между офисами вместе с устройствами (ноутбуками), в политике Агента администрирования следует создать профили подключения Агента администрирования. Профили подключения Агента администрирования поддерживают только устройства с операционными системами Windows и macOS.

Типовая конфигурация: множество небольших удаленных офисов

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

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

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

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

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

Выбор СУБД для Сервера администрирования

При выборе СУБД, используемой Сервером администрирования, следует руководствоваться количеством устройств, которые обслуживает Сервер администрирования.

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

Рекомендации и ограничения СУБД

СУБД	Рекомендации и ограничения
SQL Server Express Edition 2016 и выше	Используйте эту СУБД, если вы планируете запустить один Сервер администрирования менее чем для 10 000 устройств. Рекомендуется выключить задачу инвентаризации программного обеспечения и выключить (в параметрах политики Kaspersky Endpoint Security) уведомления Сервера администрирования о запуске приложений. Вы можете ограничить максимальное количество событий в хранилище событий, чтобы предотвратить переполнение базы данных. Дополнительную информацию см. в разделе: Расчет места в базе данных. Недопустимо совместное использование СУБД SQL Server Express Edition Сервером администрирования и какого-либо другого приложения. База данных Microsoft SQL Express не поддерживается для задачи **Синхронизация обновлений Windows Update**.
Локальный SQL Server Edition, отличный от Express, 2016 и выше	Нет ограничений.
Удаленный SQL Server Edition, отличный от Express, 2016 и выше	Допустимо только в случае, если оба устройства находятся в одном домене Windows; если домены разные, то между ними должно быть установлено двустороннее отношение доверия.
Локальный или удаленный MySQL 8.0.20 или выше	Используйте эту СУБД, если вы планируете запустить один Сервер администрирования менее чем на 50 000 устройствах. Рекомендуется выключить задачу инвентаризации программного обеспечения и выключить (в параметрах политики Kaspersky Endpoint Security) уведомления Сервера администрирования о запуске приложений. Дополнительную информацию см. в разделе: Расчет места в базе данных.

СУБД	Рекомендации и ограничения
Локальная или удаленная версия MariaDB (см. поддерживаемые версии)	Используйте эту СУБД, если вы планируете запустить один Сервер администрирования менее чем на 20 000 устройствах. Рекомендуется выключить задачу инвентаризации программного обеспечения и выключить (в параметрах политики Kaspersky Endpoint Security) уведомления Сервера администрирования о запуске приложений. Дополнительную информацию см. в разделе: Расчет места в базе данных.
PostgreSQL, Postgres Pro (см. поддерживаемые версии)	Используйте одну из этих СУБД, если вы планируете использовать один Сервер администрирования менее чем для 50 000 устройств. Рекомендуется выключить задачу инвентаризации программного обеспечения и выключить (в параметрах политики Kaspersky Endpoint Security) уведомления Сервера администрирования о запуске приложений. Дополнительную информацию см. в разделе: Расчет места в базе данных.

Если вы выбрали MSSQL 2019, вам нужно использовать накопительное исправление CU12 или выше. Чтобы избежать ошибки и перегрузки системы, которая может возникнуть.

Применение накопительного исправления CU12 при использовании SQL Server 2019 в качестве СУБД

Если вы используете SQL Server 2019 в качестве СУБД и у вас нет накопительного патча CU12 или более поздней версии, это может привести к ошибкам, например, "There is insufficient system memory in resource pool 'internal' to run this query."

После установки Kaspersky Security Center выполните следующие шаги:

1. Подключиться к SQL-серверу с помощью SQL Management Studio.
2. Выполнить следующую команду (если вы выбрали другое имя для базы данных, используйте это имя вместо KAV):

   ```
   USE KAV
   GO
   ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
   GO
   ```

3. Перезапустить службу SQL Server 2019.

Настройка сервера MariaDB x64 для работы с Kaspersky Security Center 15.1

Чтобы настроить сервер MariaDB x64 для работы с Kaspersky Security Center, необходимо использовать параметры сервера по умолчанию, если в этой статье не указаны иные параметры.
Кроме того, необходимо включить поддержку InnoDB и хранилища MEMORY, а также поддержку кодировки UTF-8.

Kaspersky Security Center 15.1 поддерживает СУБД MariaDB. Дополнительные сведения о поддерживаемых версиях MariaDB см. в разделе Аппаратные и программные требования.

Рекомендуемые параметры для файла my.ini

Чтобы настроить файл my.ini:

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

2. Добавьте следующие строки в секцию `[mysqld]` файла my.ini:

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=< 80% оперативной памяти, выделенной для СУБД; рекомендации см. в документации СУБД >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

   Обратите внимание, что память, указанная в `innodb_buffer_pool_size`, выделяется при запуске сервера. Если размер базы данных меньше указанного размера буфера, выделяется только необходимая память. Рекомендации по настройке параметра innodb_buffer_pool_size и иную дополнительную информацию см. в документации MySQL.

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

   По умолчанию для параметра `innodb_file_per_table` установлено значение `1` (ON). Убедитесь, что оно не изменено. Если значение параметра равно `0` (OFF), укажите в секции `[mysqld]` файла my.ini следующую строку:

```
innodb_file_per_table=1
```

   Для MariaDB 11.8 дополнительно введите в раздел [mysqld] следующую строку:

```
innodb_snapshot_isolation=0
```

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

Чтобы проверить, включены ли надстройки оптимизатора:

1. В клиентской консоли MariaDB выполните команду:

```
SELECT @@optimizer_switch;
```

2. Убедитесь, что вывод содержит следующие строки:

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

   Если эти строки присутствуют и содержат значение `on`, то надстройки оптимизатора включены.

Если эти строки отсутствуют или имеют значение `off`, выполните следующее:

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

2. Добавьте следующие строки в секцию `[mysqld]` файла my.ini:
```
optimizer_switch='join_cache_incremental=on'
optimizer_switch='join_cache_hashed=on'
optimizer_switch='join_cache_bka=on'
```

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

Настройка сервера MySQL x64 для работы с Kaspersky Security Center 15.1

Чтобы настроить сервер MySQL x64 для работы с Kaspersky Security Center, необходимо использовать параметры сервера по умолчанию, если в этой статье не указаны иные параметры.

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

Рекомендуемые параметры для файла my.ini

Чтобы настроить файл my.ini:

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

2. Добавьте следующие строки в секцию `[mysqld]` файла my.ini:
```
sort_buffer_size=10M
join_buffer_size=20M
tmp_table_size=600M
max_heap_table_size=600M
key_buffer_size=200M
innodb_buffer_pool_size=< 80% оперативной памяти, выделенной для СУБД; рекомендации см. в документации СУБД >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (в большинстве случаев сервер использует небольшие транзакции)
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

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

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

Настройка сервера PostgreSQL или Postgres Pro для работы с Kaspersky Security Center 15.1

Чтобы настроить сервер PostgreSQL или Postgres Pro для работы с Kaspersky Security Center, необходимо использовать параметры сервера по умолчанию, если в этой статье не указаны иные параметры.

Kaspersky Security Center 15.1 поддерживает СУБД PostgreSQL и Postgres Pro. Если вы используете одну из этих СУБД, рассмотрите возможность настройки параметров сервера СУБД для оптимизации работы СУБД с Kaspersky Security Center.

Рекомендуемые параметры для PostgreSQL и Postgres Pro:

- `max_connections = 151`
- `shared_buffers = N`

  N = 25 процентов от объема оперативной памяти устройства, на котором установлена СУБД. Если оперативной памяти меньше 1 ГБ, то оставьте значение по умолчанию.
- `temp_buffers = 24MB`
- `work_mem = 16MB`
- `maintenance_work_mem = 128MB`
- `max_stack_depth = 2MB`
- `max_parallel_workers_per_gather = 0`
- `standard_conforming_strings = on`

После обновления конфигурационного файла примените конфигурацию или перезапустите службу СУБД.

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

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

Управление мобильными устройствами с установленным Kaspersky Endpoint Security для Android

Управление мобильными устройствами с установленным приложением Kaspersky Endpoint Security для Android™ (далее KES-устройства) осуществляется с помощью Сервера администрирования. Kaspersky Security Center поддерживает следующие возможности управления KES-устройствами:

- работа с мобильными устройствами как с клиентскими устройствами:
  - членство в группах администрирования;
  - мониторинг, например просмотр статусов, событий и отчетов;
  - изменение локальных параметров и назначение политик для приложения Kaspersky Endpoint Security для Android;
- централизованная отправка команд;
- удаленная установка пакетов мобильных приложений.

Сервер администрирования управляет KES-устройствами по протоколу TLS, TCP-порт 13292.

Предоставление доступа к Серверу администрирования из интернета

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

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

  По умолчанию Сервер администрирования не требует подключения к интернету для установки обновлений приложений Microsoft на управляемые устройства. Например, управляемые устройства могут загружать обновления приложений Microsoft непосредственно с серверов обновлений Microsoft или с Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации. Сервер администрирования должен быть подключен к интернету в следующих случаях:
  - Когда вы используете Сервер администрирования в роли WSUS-сервера.
  - Для установки обновлений приложений сторонних производителей, отличных от приложений Microsoft.
- Закрытие уязвимостей в приложениях сторонних производителей

  Подключение Сервера администрирования к интернету необходимо для выполнения следующих задач:
  - Составление списка рекомендуемых исправлений уязвимостей в приложениях Microsoft. Список формируется и регулярно обновляется специалистами "Лаборатории Касперского".
  - Закрытие уязвимостей в приложениях сторонних производителей, отличных от приложений Microsoft.
- Для управления устройствами (ноутбуками) автономных пользователей.
- Для управления устройствами, находящимися в удаленных офисах.

- При взаимодействии с главным или подчиненными Серверами администрирования, находящимися в удаленных офисах.

- Для управления мобильными устройствами.

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

Доступ из интернета: Сервер администрирования в локальной сети

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

Доступ из интернета: Сервер администрирования в демилитаризованной зоне

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

- Сервер администрирования не может самостоятельно обнаруживать новые устройства.

- Сервер администрирования не может выполнять первоначальное развертывание Агента администрирования посредством принудительной установки на устройства внутренней сети организации.

Речь идет только о первоначальной установке Агента администрирования. Последующие обновления версии Агента администрирования или установка приложения безопасности уже могут быть выполнены Сервером администрирования. Однако первоначальное развертывание Агентов администрирования может быть выполнено иными средствами, например, при помощи групповых политик Microsoft Active Directory.

- Сервер администрирования не может посылать управляемым устройствам уведомления на порт 15000 UDP, что не является критичным для работы Kaspersky Security Center.

- Сервер администрирования не может опрашивать Active Directory. Однако результаты опроса Active Directory не нужны в большинстве сценариев.

Если описанные выше ограничения критичны, они могут быть сняты при помощи точек распространения, размещенных в сети организации:

- Для выполнения первоначального развертывания на устройствах без Агента администрирования следует предварительно установить Агент администрирования на одно из устройств и назначить это устройство точкой распространения. В результате первоначальная установка Агента администрирования на прочие устройства будет выполняться Сервером администрирования через эту точку распространения.

- Для обнаружения новых устройств во внутренней сети организации и для опроса Active Directory следует на одной из точек распространения включить желаемые виды опроса сети.

Для успешной отправки уведомлений управляемым устройствам, размещенным во внутренней сети организации, на порт 15000 UDP, следует покрыть всю сеть предприятия точками распространения. В свойствах назначенных точек распространения установите флажок **Не разрывать соединение с Сервером администрирования**. В результате Сервер администрирования будет иметь постоянную связь с точками распространения, а точки распространения смогут посылать уведомления на порт 15000 UDP устройствам, размещенным во внутренней сети организации (это может быть IPv4-сеть или IPv6-сеть).

Доступ из интернета: Агент администрирования в качестве шлюза соединения в демилитаризованной зоне

Сервер администрирования может располагаться во внутренней сети организации, а в демилитаризованной зоне сети может находиться устройство с Агентом администрирования, работающим в качестве шлюза соединения с обратным направлением подключения (Сервер администрирования устанавливает соединение с Агентом администрирования). В этом случае для организации доступа из интернета нужно выполнить следующие условия:

- На устройство, находящееся в демилитаризованной зоне, следует установить Агент администрирования. При установке Агента администрирования в окне **Шлюз соединения** мастера установки выберите **Использовать в качестве шлюза соединения в демилитаризованной зоне**.

- Устройство с установленным шлюзом соединения необходимо добавить в качестве точки распространения. Когда вы добавляете шлюз соединения, в окне **Добавление точки распространения** выберите параметр **Выбрать → Добавить шлюз соединений, находящийся в демилитаризованной зоне, по адресу**.

- Для того чтобы использовать интернет для подключения внешних настольных устройств к Серверу администрирования, необходимо изменить инсталляционный пакет Агента администрирования. В свойствах созданного инсталляционного пакета выберите параметр **Дополнительно →Подключаться к Серверу администрирования через шлюз соединения** и укажите вновь созданный шлюз соединения.

Для шлюза соединений, находящегося в демилитаризованной зоне, Сервер администрирования создает сертификат, подписанный сертификатом Сервера администрирования. Если администратор принял решение задать Серверу администрирования пользовательский сертификат, то это следует сделать до создания шлюза соединений в демилитаризованной зоне.

При наличии сотрудников с ноутбуками, которые могут подключаться к Серверу администрирования как из локальной сети, так и из интернета, может быть целесообразно создать в политике Агента администрирования правило переключения Агента администрирования.

О точках распространения

Устройства с установленным Агентом администрирования могут быть использованы в качестве точки распространения. В этом режиме Агент администрирования может выполнять следующие функции:

- Раздавать обновления, причем обновления могут быть получены как с Сервера администрирования, так и с серверов "Лаборатории Касперского". В последнем случае для устройства, являющегося точкой распространения, должна быть создана задача *Загрузка обновлений в хранилища точек распространения*.

  - Устанавливать программное обеспечение на другие устройства, в том числе выполнять первоначальное развертывание Агентов администрирования на устройствах.

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

Размещение точек распространения в сети организации преследует следующие цели:

- Уменьшение нагрузки на Сервер администрирования.

- Оптимизация трафика.

- Предоставление Серверу администрирования доступ к устройствам в труднодоступных частях сети организации. Наличие точки распространения в находящейся за NAT (по отношению к Серверу администрирования) сети позволяет Серверу администрирования выполнять следующие действия:
  - отправлять уведомления на устройства через UDP в IPv4-сети или IPv6-сети;
  - опрашивать IPv4-сети или IPv6-сети;
  - выполнять первоначальное развертывание;
  - использовать в качестве push-сервера.

Точка распространения назначается на группу администрирования. В этом случае областью действия точки распространения будут устройства, находящиеся в этой группе администрирования и всех ее подгруппах. При этом устройство, являющееся точкой распространения, не обязано находиться в группе администрирования, на которую она назначена.

Вы можете сделать точку распространения шлюзом соединений. В этом случае, устройства, находящиеся в области действия точки распространения, будут подключаться к Серверу администрирования не напрямую, а через шлюз. Данный режим полезен в сценариях, когда между Сервером администрирования и управляемыми устройствами невозможно прямое соединение.

Если вы используете устройство под управлением Linux в качестве точки распространения, настоятельно рекомендуется увеличить ограничения дескрипторов файлов для службы klnagent, так как, если в область действия точки распространения входит много устройств, может не хватить максимального количества файлов, которые могут быть открыты по умолчанию.

Увеличение ограничения дескрипторов файлов для службы klnagent

Если область распространения точки распространения под управлением Linux включает в себя большое количество устройств, ограничения на количество открываемых файлов (дескрипторов файлов), которое было установлено по умолчанию, может быть недостаточно. Чтобы этого избежать, вы можете увеличить ограничение дескрипторов файлов для службы klnagent.

Чтобы увеличить ограничение дескрипторов файлов для службы klnagent

1. На устройстве с операционной системой Linux, выполняющем роль точки распространения, выполните следующую команду:

   ```
   systemctl edit klnagent64.service
   ```

2. Укажите жесткие и мягкие ограничения файловых дескрипторов в параметре `LimitNOFILE` в секции `[Service]`:

   ```
   LimitNOFILE=<soft resource limits>:<hard resource limits>
   ```

   Например, `LimitNOFILE=32768:131072`. Обратите внимание, что мягкие ограничения дескрипторов файлов должны быть меньше или равны жесткому ограничению.

3. Выполните следующую команду, чтобы убедиться, что параметры указаны правильно:

   ```
   systemd-analyze verify klnagent64.service
   ```

Если параметры указаны неверно, эта команда может вывести одну из следующих ошибок:

- `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

  Если эта ошибка возникла, значит, символы в строке `LimitNOFILE` указаны неверно. Вам нужно проверить и исправить введенную строку.

- `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

  Если эта ошибка возникла, мягкое ограничение введенных вами дескрипторов файлов превышает жесткое ограничение. Вам нужно проверить введенную строку и убедиться, что мягкое ограничение дескрипторов файлов меньше или равно жесткому ограничению.

4. Выполните следующую команду, чтобы перезагрузить процесс systemd:

   ```
   systemctl daemon-reload
   ```

5. Выполните следующую команду, чтобы перезапустить службу Агента администрирования:

   ```
   systemctl restart klnagent
   ```

6. Выполните следующую команду, чтобы убедиться, что указанные параметры применяются правильно:

   ```
   less /proc/<nagent process id>/limits
   ```

   где параметр `<nagent process id>` является идентификатором процесса Агента администрирования. Вы можете выполнить следующую команду, чтобы получить идентификатор:

   ```
   ps -ax | grep klnagent
   ```

Для точки распространения с операционной системой Linux количество открываемых файлов увеличено.

Расчет количества и конфигурации точек распространения

Чем больше клиентских устройств содержит сеть, тем больше требуется точек распространения. Рекомендуется не отключать автоматическое назначение точек распространения. При включенном автоматическом назначении точек распространения Сервер администрирования назначает точки распространения, если число клиентских устройств достаточно велико, и определяет их конфигурацию.

Использование специально выделенных точек распространения

Если вы планируете использовать в качестве точек распространения какие-то определенные устройства (например, выделенные для этого серверы), то можно не использовать автоматическое назначение точек распространения. В этом случае убедитесь, что устройства, которые вы хотите назначить точками распространения, имеют достаточно свободного места на диске, их не отключают регулярно и на них выключен "спящий режим".

Число специально выделенных точек распространения в сети, содержащей один сегмент сети, в зависимости от количества устройств в сети

Число клиентских устройств в сегменте сети	Количество точек распространения
Менее 300	0 (точки распространения не нужны)
Более 300	Приемлемо: (N/10 000 + 1), рекомендуется: (N/5000 + 2), где N количество устройств в сети

Число специально выделенных точек распространения в сети, содержащей несколько сегментов сети, в зависимости от количества устройств в сети

Число клиентских устройств в каждом сегменте сети	Количество точек распространения
Менее 10	0 (точки распространения не нужны)
10–100	1
Более 100	Приемлемо: (N/10 000 + 1), рекомендуется: (N/5000 + 2), где N количество устройств в сети

Использование клиентских устройств (рабочих станций) в качестве точек распространения

Если вы планируете использовать в качестве точек распространения обычное клиентское устройство (рабочую станцию), то рекомендуется назначать точку распространения, как показано в таблице ниже, чтобы избежать чрезмерной нагрузки на каналы связи и Сервер администрирования:

Число рабочих станций, выполняющих роль точек распространения в сети, которая содержит один сегмент сети, в зависимости от количества сетевых устройств

Число клиентских устройств в сегменте сети	Количество точек распространения
Менее 300	0 (точки распространения не нужны)
Более 300	(N/300 +1), где N – число устройств в сети; не менее 3 точек распространения

Число рабочих станций, выполняющих роль точек распространения в сети, которая содержит несколько сегментов сети, в зависимости от количества сетевых устройств

Число клиентских устройств в каждом сегменте сети	Количество точек распространения
Менее 10	0 (точки распространения не нужны)
10–30	1
31–300	2
Более 300	(N/300 +1), где N – число устройств в сети; не менее 3 точек распространения

Если точка распространения отключена или по другим причинам недоступна, то управляемые устройства из области действия этой точки распространения могут обращаться за обновлениями к Серверу администрирования.

Иерархия Серверов администрирования

У MSP может быть более одного Сервера администрирования. Администрировать несколько разрозненных Серверов неудобно, поэтому целесообразно объединять их в иерархию. Взаимодействие "главный – подчиненный" между двумя Серверами администрирования предоставляет следующие возможности:

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

Главный Сервер администрирования получает данные только от невиртуальных подчиненных Серверов администрирования в рамках перечисленных выше параметров. Это ограничение не распространяется на виртуальные Серверы администрирования, которые совместно используют базу данных со своим главным Сервером администрирования.

Виртуальные Серверы администрирования

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

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

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

Информация об ограничениях Kaspersky Security Center

В таблице ниже приведены ограничения текущей версии Kaspersky Security Center.

Ограничения Kaspersky Security Center

Тип ограничения	Значение
Максимальное количество управляемых устройств на один Сервер администрирования	100 000
Максимальное количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**	300
Максимальное количество групп администрирования	10 000
Максимальное количество хранимых событий	45 000 000
Максимальное количество политик	2000
Максимальное количество задач	2000
Максимальное суммарное количество объектов Active Directory (подразделений и учетных записей пользователей, устройств и групп безопасности)	1 000 000
Максимальное количество профилей в политике	100
Максимальное количество подчиненных Серверов у одного главного Сервера администрирования	500
Максимальное количество виртуальных Серверов администрирования	500
Максимальное количество устройств, которые может обслуживать одна точка распространения (точки распространения могут обслуживать только немобильные устройства)	10 000

Тип ограничения	Значение
Максимальное количество устройств, которые могут использовать один шлюз соединения	10 000, включая мобильные устройства
Максимальное количество мобильных устройств на один Сервер администрирования	100 000 минус количество стационарных управляемых устройств

Нагрузка на сеть

В этом разделе приводится информация об объеме сетевого трафика, которым обмениваются между собой клиентские устройства и Сервер администрирования в ходе выполнения ключевых административных сценариев.

Основная нагрузка на сеть связана с выполнением следующих административных сценариев:

- Первоначальное развертывание антивирусной защиты
- Первоначальное обновление антивирусных баз
- Синхронизация клиентского устройства с Сервером администрирования
- Регулярное обновление антивирусных баз
- Обработка событий на клиентских устройствах Сервером администрирования

Первоначальное развертывание антивирусной защиты

В этом разделе приведен расход трафика при установке на клиентском устройстве Агента администрирования версии и Kaspersky Endpoint Security для Windows (см. таблицу ниже).

Агент администрирования устанавливается путем принудительной установки, когда требуемые для установки файлы копируются Сервером администрирования в папку общего доступа на клиентском устройстве. После установки Агент администрирования получает дистрибутив Kaspersky Endpoint Security для Windows, используя соединение с Сервером администрирования.

Расход трафика

Сценарий	Установка Агента администрирования для одного клиентского устройства	Установка Kaspersky Endpoint Security для Windows для одного клиентского устройства (с обновленными базами)	Совместная установка Агента администрирования и Kaspersky Endpoint Security для Windows
Трафик от клиентского устройства к Серверу администрирования, КБ	1638,4	7843,84	9707,52
Трафик от Сервера администрирования к клиентскому устройству, КБ	69 990,4	259 317,76	329 318,4
Общий трафик (для одного клиентского устройства), КБ	71 628,8	267 161,6	339 025,92

После установки Агентов администрирования на клиентские устройства можно назначить одно из устройств в группе администрирования точкой распространения. Он будет использоваться для распространения инсталляционных пакетов. В этом случае объем трафика, передаваемого при первоначальном развертывании антивирусной защиты, существенно отличается в зависимости от того, используется ли многоадресная IP-рассылка.

В случае использования многоадресной IP-рассылки инсталляционные пакеты рассылаются один раз по всем включенным устройствам в группе администрирования. Таким образом, общий трафик уменьшится примерно в N раз, где N – общее число включенных устройств в группе администрирования. Если многоадресная IP-рассылка не используется, общий трафик совпадает с трафиком загрузки дистрибутивов с Сервера администрирования. При этом источником инсталляционных пакетов является точка распространения, а не Сервер администрирования.

Первоначальное обновление антивирусных баз

Скорости трафика при первичном обновлении антивирусных баз (при первом запуске задачи обновления баз на клиентском устройстве) следующие:

- Трафик от клиентского устройства к Серверу администрирования: 1.8 МБ.
- Трафик от Сервера администрирования к клиентскому устройству: 113 МБ.
- Общий трафик (для одного клиентского устройства): 114 МБ.

Данные могут несколько отличаться в зависимости от текущей версии антивирусных баз.

Синхронизация клиента с Сервером администрирования

Этот сценарий характеризует состояние системы администрирования в случае, когда происходит активная синхронизация данных между клиентским устройством и Сервером администрирования. Клиентские устройства подключаются к Серверу администрирования с периодом, заданным администратором. Сервер администрирования сравнивает состояние данных на клиентском устройстве с состоянием данных на Сервере, регистрирует данные о последнем подключении клиентского устройства в базе данных и проводит синхронизацию данных.

В разделе приведена информация о расходе трафика для основных административных сценариев при подключении клиента к Серверу администрирования с синхронизацией (см. таблицу ниже). Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии антивирусных баз.

Расход трафика

Сценарий	Трафик от клиентских устройств к Серверу администрирования, КБ	Трафик от Сервера администрирования к клиентским устройствам, КБ	Общий трафик (для одного клиентского устройства), КБ
Первоначальная синхронизация до обновления баз на клиентском устройстве	699,44	568,42	1267,86
Первоначальная синхронизация после обновления баз на клиентском устройстве	735,8	4474,88	5210,68
Синхронизация при отсутствии изменений на клиентском устройстве и на Сервере администрирования	11,99	6,73	18,72
Синхронизация при изменении одного параметра в политике группы	9,79	11,39	21,18
Синхронизация при изменении одного параметра в групповой задаче	11,27	11,72	22,99
Принудительная синхронизация при отсутствии изменений на клиентском устройстве	77,59	99,45	177,04

Объем общего трафика существенно изменяется в зависимости от того, используется ли многоадресная IP-рассылка внутри групп администрирования. В случае использования многоадресной IP-рассылки общий трафик для группы уменьшается примерно в N раз, где N – число включенных устройств в группе администрирования.

Объем трафика при первоначальной синхронизации до и после обновления баз указан для следующих случаев:

- установка на клиентское устройство Агента администрирования и приложения безопасности;
- перенос клиентского устройства в группу администрирования;
- применение к клиентскому устройству политики и задач, созданных для группы по умолчанию.

В таблице указан объем трафика при изменении одного из параметров защиты, входящих в параметры политики Kaspersky Endpoint Security. Данные для других параметров политики могут отличаться от данных, представленных в таблице.

Дополнительное обновление антивирусных баз

Расход трафика при инкрементальном обновлении антивирусных баз спустя 20 часов после предыдущего обновления следующий:

- Трафик от клиентского устройства к Серверу администрирования: 169 КБ.
- Трафик от Сервера администрирования к клиентскому устройству: 16 МБ.
- Общий трафик (для одного клиентского устройства): 16.3 МБ.

Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии антивирусных баз.

Объем трафика существенно изменяется в зависимости от того, используется ли многоадресная IP-рассылка внутри групп администрирования. В случае использования многоадресной IP-рассылки общий трафик для группы уменьшается примерно в N раз, где N – число включенных устройств в группе администрирования.

Обработка событий клиентов Сервером администрирования

В этом разделе приведен расход трафика при возникновении на клиентском устройстве события "Найден вирус", информация о котором передается на Сервер администрирования и регистрируется в базе данных (см. таблицу ниже).

Расход трафика

Сценарий	Передача на Сервер администрирования данных при наступлении события "Найден вирус"	Передача на Сервер администрирования данных при наступлении девяти событий "Найден вирус"
Трафик от клиентского устройства к Серверу администрирования, КБ	49,66	64,05
Трафик от Сервера администрирования к клиентскому устройству, КБ	28,64	31,97
Общий трафик (для одного клиентского устройства), КБ	78,3	96,02

Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии антивирусного приложения и в зависимости от того, какие именно события определены в политике как требующие регистрации в базе данных Сервера администрирования.

Расход трафика за сутки

В этом разделе приведена информация о расходе трафика за сутки работы системы администрирования в состоянии "покоя", когда не происходит изменений данных ни со стороны клиентских устройств, ни со стороны Сервера администрирования (см. таблицу ниже).

Данные, приведенные в таблице, характеризуют состояние сети после стандартной установки Kaspersky Security Center и завершения работы мастера первоначальной настройки. Период синхронизации клиентского устройства с Сервером администрирования составлял 20 минут, загрузка обновлений в хранилище Сервера администрирования происходила каждый час.

Уровень трафика за сутки в состоянии простоя

Поток трафика	Значение
Трафик от клиентского устройства к Серверу администрирования, КБ	3235,84
Трафик от Сервера администрирования к клиентскому устройству, КБ	64 378,88
Общий трафик (для одного клиентского устройства), КБ	67 614,72

Подготовка к управлению мобильными устройствами

Этот раздел содержит информацию:

- о сервере iOS MDM для управления iOS-устройствами путем установки на них специализированных iOS MDM-профилей;
- об управлении мобильными устройствами с установленным приложением Kaspersky Endpoint Security для Android.

Сервер iOS MDM

Сервер iOS MDM позволяет осуществлять управление iOS-устройствами путем установки на них специализированных iOS MDM-профилей. Поддерживаются следующие функции:

- блокирование устройства;
- сброс пароля;
- удаление данных устройства;
- установка или удаление приложений;
- применение iOS MDM-профиля с дополнительными параметрами (такими как параметры VPN, почты, Wi-Fi, камеры, сертификаты, и так далее).

Сервер iOS MDM представляет собой веб-службу, которая принимает входящие соединения от мобильных устройств на свой TLS-порт (по умолчанию порт 443) и управляется со стороны Kaspersky Security Center с помощью Агента администрирования. Агент администрирования устанавливается локально на устройстве с развернутым Сервером iOS MDM.

В процессе развертывания Сервера iOS MDM администратору необходимо выполнить следующие действия:

- обеспечить Агенту администрирования доступ к Серверу администрирования;
- обеспечить мобильным устройствам доступ к TCP-порту Сервера iOS MDM.

В этом разделе рассмотрены две типовые конфигурации Сервера iOS MDM.

Типовая конфигурация: Kaspersky Device Management для iOS в демилитаризованной зоне

Сервер iOS MDM располагается в демилитаризованной зоне сети организации с доступом в интернет. Особенностью данного подхода является отсутствие проблем с доступностью веб-службы iOS MDM из интернета со стороны устройств.

Так как для управления Сервером iOS MDM требуется локально установленный Агент администрирования, необходимо обеспечить взаимодействие этого Агента администрирования с Сервером администрирования. Это можно сделать следующими способами:

- Поместить Сервер администрирования в демилитаризованную зону.
- Использовать шлюз соединений:
    a. На устройстве с развернутым Сервером iOS MDM подключить Агент администрирования к Серверу администрирования через шлюз соединений.
    b. На устройстве с развернутым Сервером iOS MDM назначить Агент администрирования шлюзом соединений.

Типовая конфигурация: Сервер iOS MDM в локальной сети организации

Сервер iOS MDM располагается во внутренней сети организации. Порт 443 (порт по умолчанию) должен быть доступным извне, например, путем публикации веб-службы iOS MDM на обратном прокси-сервере, который поддерживает использование Kerberos Constrained Delegation.

В любой типовой конфигурации потребуется обеспечить доступность для Сервера iOS MDM веб-сервисов Apple (диапазон адресов 17.0.0.0/8) по порту TCP 2197. Этот порт используется для оповещения устройств о новых командах через специализированный сервис APNs.

Управление мобильными устройствами с установленным Kaspersky Endpoint Security для Android

Управление мобильными устройствами с установленным приложением Kaspersky Endpoint Security для Android™ (далее KES-устройства) осуществляется с помощью Сервера администрирования. Kaspersky Security Center поддерживает следующие возможности управления KES-устройствами:

- работа с мобильными устройствами как с клиентскими устройствами:
    - членство в группах администрирования;
    - мониторинг, например просмотр статусов, событий и отчетов;
    - изменение локальных параметров и назначение политик для приложения Kaspersky Endpoint Security для Android;
- централизованная отправка команд;
- удаленная установка пакетов мобильных приложений.

Сервер администрирования управляет KES-устройствами по протоколу TLS, TCP-порт 13292.

Сведения о производительности Сервера администрирования

В разделе представлены результаты тестирования производительности Сервера администрирования для разных аппаратных конфигураций, а также ограничения на подключение управляемых устройств к Серверу администрирования.

Ограничения подключений к Серверу администрирования

Сервер администрирования поддерживает управление до 100 000 устройств без потери производительности.

Ограничения на подключения к Серверу администрирования без потери производительности:

- Один Сервер администрирования может поддерживать до 500 виртуальных Серверов администрирования.
- Главный Сервер администрирования поддерживает одновременно не более 1000 сеансов.
- Виртуальные Серверы администрирования поддерживают одновременно не более 1000 сеансов.

Результаты тестов производительности Сервера администрирования

Результаты тестов производительности Сервера администрирования позволили определить максимальные количества клиентских устройств, с которыми Сервер администрирования может выполнить синхронизацию за указанные промежутки времени. Вы можете использовать эту информацию для выбора оптимальной схемы развертывания антивирусной защиты в компьютерных сетях.

Для тестирования использовались устройства со следующими аппаратными конфигурациями (см. таблицы ниже):

Аппаратная конфигурация Сервера администрирования

Параметр	Значение
Процессор	Intel Xeon CPU E5630, тактовая частота 2,53 ГГц, 2 сокет, 8 ядер, 16 логических процессоров
ОЗУ	26 ГБ
Жесткий диск	IBM ServeRAID M5014 SCSI Disk Device, 487 ГБ
Операционная система	Microsoft Windows Server 2019 Standard, версия 10.0.17763, сборка 17763
Сеть	QLogic BCM5709C Gigabit Ethernet (NDIS VBD Client)

Аппаратная конфигурация устройства с SQL Server

Параметр	Значение
Процессор	Intel Xeon CPU X5570, тактовая частота 2,93 ГГц, 2 сокет, 8 ядер, 16 логических процессоров
ОЗУ	32 ГБ
Жесткий диск	Adaptec Array SCSI Disk Device, 2047 ГБ
Операционная система	Microsoft Windows Server 2019 Standard, версия 10.0.17763, сборка 17763
Сеть	Intel 82576 Gigabit

Сервер администрирования поддерживал создание 500 виртуальных Серверов администрирования.

Период синхронизации составлял по 15 минут на каждые 10 000 управляемых устройств (см. таблицу ниже).

Обобщенные результаты нагрузочного тестирования Сервера администрирования

Период синхронизации, мин	Количество управляемых устройств
15	10 000
30	20 000
45	30 000
60	40 000
75	50 000
90	60 000
105	70 000
120	80 000
135	90 000
150	100 000

При подключении Сервера администрирования к серверу базы данных MySQL и SQL Express не рекомендуется использовать приложение для управления более чем 10 000 устройств. Для системы управления базами данных MariaDB максимальное рекомендуемое количество управляемых устройств составляет 20 000.

Результаты тестирования производительности прокси-сервера KSN

Если ваша корпоративная сеть включает в себя большое количество клиентских устройств, и они используют Сервер администрирования в качестве прокси-сервера KSN, Сервер администрирования должен удовлетворять определенным аппаратным требованиям, чтобы обрабатывать запросы с клиентских устройств. Вы можете использовать результаты тестирования ниже для оценки загрузки Сервера администрирования в вашей сети и планирования аппаратных ресурсов, для обеспечения нормальной работы службы прокси-сервера KSN.

В таблице ниже приведена конфигурация аппаратного обеспечения Сервера администрирования и SQL Server. Эта конфигурация была использована для тестирования.

Аппаратная конфигурация Сервера администрирования

Параметр	Значение
Процессор	Intel Xeon CPU E5450, тактовая частота 3,00 ГГц, 2 сокет, 8 ядер, 16 логических процессоров
ОЗУ	32 ГБ
Операционная система	Microsoft Windows Server 2016 Standard

Аппаратная конфигурация SQL Server

Параметр	Значение
Процессор	Intel Xeon CPU E5450, тактовая частота 3,00 ГГц, 2 сокет, 8 ядер, 16 логических процессоров
ОЗУ	32 ГБ
Операционная система	Microsoft Windows Server 2019 Standard

В таблице ниже приведены результаты тестирования.

Обобщенные результаты тестирования производительности прокси-сервера KSN

Параметр	Значение
Максимальное количество обработанных запросов в секунду	4914
Максимальное использование процессора	36%

Сетевые параметры для взаимодействия с внешними сервисами

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

Сетевые параметры

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 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.

Сетевые параметры	Адрес	Описание
Порт: 80 Протокол: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Эти серверы являются частью инфраструктуры открытых ключей (PKI) и необходимы для проверки статуса действительности сертификатов цифровой подписи "Лаборатории Касперского". CRL является списком отозванных сертификатов. OCSP позволяет запрашивать статус конкретного сертификата в режиме реального времени. Эти службы помогают обеспечить безопасность взаимодействия с цифровыми сертификатами и защитить от возможных атак.
Порт: 443 Протокол: HTTPS	https://ipm-klca.kaspersky.com	Рекламные объявления.

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

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

1. Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Если вы хотите загружать обновления по протоколу HTTP, выполните одну из следующих команд:

   - На устройстве, на котором установлен Сервер администрирования:

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

   - На точку распространения:

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

   Если вы хотите загружать обновления по протоколу HTTPS, выполните одну из следующих команд:

   - На устройстве, на котором установлен Сервер администрирования:

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

   - На точку распространения:

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

Развертывание Агента администрирования и приложения безопасности

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

В Microsoft Windows XP Агент администрирования может некорректно выполнять следующие операции: загрузка обновлений напрямую с серверов "Лаборатории Касперского" (если выполняет роль точки распространения); функционирование в качестве прокси-сервера KSN (если выполняет роль точки распространения); и обнаружение уязвимостей приложений сторонних производителей (при использовании Системного администрирования).

Первоначальное развертывание

Для управления устройствами организации требуется установить на устройства Агент администрирования.

Установка Агента администрирования на управляемое устройство под управлением операционной системы Windows может быть выполнена следующими способами:

- С помощью сторонних средств удаленной установки приложений.
- Путем клонирования образа жесткого диска с операционной системой и установленным Агентом администрирования: средствами, предоставляемыми Kaspersky Security Center для работы с образами дисков, или сторонними средствами.
- Через механизм групповых политик Microsoft Windows: с помощью штатных средств управления групповыми политиками Microsoft Windows или автоматизированно, с помощью соответствующего параметра в задаче удаленной установки приложений Kaspersky Security Center.
- Принудительно с использованием ресурсов операционной системы с помощью задачи удаленной установки Kaspersky Security Center.
- Путем рассылки пользователям устройств ссылок на автономные пакеты, сформированные Kaspersky Security Center. Автономные пакеты представляют собой исполняемые модули, содержащие в себе дистрибутивы выбранных приложений с настроенными параметрами.
- Вручную, запуская инсталляторы приложений на устройствах.

Первоначальная установка Агента администрирования на управляемое устройство с операционной системой Linux может быть выполнена следующими способами:

- Подключиться к управляемому устройству с помощью SSH и запустить задачу удаленной установки.
- Запустить установку инсталляционного пакета на управляемом устройстве.

Первоначальная установка Агента администрирования на управляемое устройство с операционной системой macOS может быть выполнена следующими способами:

- Запустить задачу удаленной установки с помощью точки распространения с операционной системой macOS.

- Отправить пользователям устройств ссылки на автономные пакеты, сформированные Kaspersky Security Center. Автономные пакеты представляют собой исполняемые модули, содержащие в себе дистрибутивы выбранных приложений с настроенными параметрами.

После установки Агента администрирования на устройство вы можете выполнять удаленную установку приложений "Лаборатории Касперского" на устройстве с помощью этого Агента администрирования. При этом передача дистрибутива устанавливаемого приложения вместе с заданными администратором инсталляционными параметрами осуществляется по каналам связи между Агентами администрирования и Сервером администрирования. Для передачи дистрибутива можно использовать промежуточные центры распространения в виде точек распространения, многоадресную рассылку и прочие средства.

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

- конфигурацию сети организации;

- общее количество устройств;

- наличие в сети организации устройств, не являющихся членами доменов Active Directory, и наличие унифицированных учетных записей с административными правами на таких устройствах;

- ширину канала между Сервером администрирования и устройствами;

- тип связи между Сервером администрирования и удаленными подсетями и ширину сетевых каналов внутри таких подсетей;

- параметры безопасности, примененные к удаленным устройствам на момент начала развертывания. Эти параметры позволяют установить удаленное подключение с управляемым устройством и начать установку.

Настройка параметров инсталляторов

Прежде чем приступать к развертыванию в сети приложений "Лаборатории Касперского", следует определить параметры инсталляции – те параметры, которые настраиваются в ходе установки приложения. При установке Агента администрирования требуется задать по крайней мере адрес для подключения к Серверу администрирования, а возможно, и некоторые дополнительные параметры. В зависимости от выбранного способа установки параметры можно задавать различными способами. В простейшем случае (при интерактивной установке вручную на выбранное устройство) необходимые параметры можно задать с помощью пользовательского интерфейса инсталлятора.

Этот способ настройки параметров не подходит для тихой установки приложений на группы устройств. В типичном случае администратор должен централизованно указать значения параметров, которые в дальнейшем могут быть использованы для тихой установки на выбранные устройства в сети.

Инсталляционные пакеты

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

Инсталляционные пакеты создаются следующими способами:

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

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

Значения параметров инсталляции, специфичные для конкретного поддерживаемого приложения, можно задавать в пользовательском интерфейсе Консоли администрирования при создании инсталляционного пакета. В случае удаленной установки приложений средствами Kaspersky Security Center инсталляционные пакеты доставляются на устройства таким образом, что при запуске инсталлятора приложения ему становятся доступны все заданные администратором параметры. При использовании сторонних средств установки приложений "Лаборатории Касперского" достаточно обеспечить доступность на устройстве всего инсталляционного пакета, то есть дистрибутива и его параметров. Инсталляционные пакеты создаются и хранятся Kaspersky Security Center в соответствующей подпапке папки общего доступа.

Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.

О том, как именно можно воспользоваться этим способом настройки параметров для приложений "Лаборатории Касперского" перед их развертыванием сторонними средствами, см. в разделе "Развертывание с помощью механизма групповых политик Microsoft Windows".

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

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

Свойства MSI и файлы трансформации

Другим способом настроить параметры инсталляции на платформе Windows является задание свойств MSI и файлов трансформации. Этот способ может быть использован в следующих случаях:

- при установке через групповые политики Windows при помощи штатных средств Microsoft или иных сторонних инструментов для работы с групповыми политиками Windows;
- при установке с помощью сторонних средств, ориентированных на работу с инсталляторами в формате Microsoft Installer.

Развертывание при помощи сторонних средств удаленной установки приложений

При наличии в организации каких-либо средств удаленной установки приложений (например, Microsoft System Center) целесообразно выполнять первоначальное развертывание при помощи этих средств.

Нужно выполнить следующие действия:

- Выбрать способ настройки параметров инсталляции, наиболее подходящий для используемого средства развертывания.
- Определить механизм синхронизации между изменением параметров инсталляционных пакетов через интерфейс Консоли администрирования и работой выбранных сторонних средств развертывания приложений из данных инсталляционных пакетов.
- В случае установки из папки общего доступа убедиться в достаточной производительности этого файлового ресурса.

О задачах удаленной установки приложений Kaspersky Security Center

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

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

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

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

Развертывание захватом и копированием образа устройства

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

Чтобы выполнить развертывание путем захвата и копирования жесткого диска:

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

2. Захватить образ "эталонного" устройства и далее распространять этот образ на новые устройства посредством задачи Kaspersky Security Center.

   Для захвата и установки образов диска можно воспользоваться как имеющимися в организации сторонними средствами, так и функциональностью, предоставляемой (при наличии лицензии на Системное администрирование) Kaspersky Security Center.

Если для работы с образами диска используются сторонние инструменты, необходимо при развертывании на устройство из эталонного образа обеспечить удаление информации, с помощью которой Kaspersky Security Center идентифицирует управляемое устройство. В противном случае Сервер администрирования не сможет в дальнейшем корректно различать устройства, созданные путем копирования одного и того же образа.

При захвате образа диска средствами Kaspersky Security Center эта проблема решается автоматически.

Копирование образа жесткого диска сторонними инструментами

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

- Рекомендуемый метод. При установке Агента администрирования на эталонное устройство захватить образ устройства до первого запуска службы Агента администрирования (так как уникальная информация, идентифицирующая устройство, создается при первом подключении Агента администрирования к Серверу администрирования). В дальнейшем рекомендуется не допускать запуск службы Агента администрирования вплоть до выполнения операции захвата образа.

- На эталонном устройстве остановить службу Агента администрирования и запустить утилиту klmover с ключом -dupfix. Утилита klmover входит в состав инсталляционного пакета Агента администрирования. В дальнейшем не допускать запуск службы Агента администрирования вплоть до выполнения операции захвата образа.

- Обязательно запускать утилиту klmover с ключом -dupfix до первого запуска службы Агента администрирования на устройствах при первом запуске операционной системы после развертывания образа. Утилита klmover входит в состав инсталляционного пакета Агента администрирования.

- Использовать режим клонирования диска Агента администрирования.

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

Также можно захватить образ устройства без установленного Агента администрирования. Для этого выполните развертывание образа на целевых устройствах, а затем установите Агент администрирования. При использовании этого метода предоставьте доступ к сетевой папке с автономными инсталляционными пакетами с устройства.

Неверно выполнено копирование образа жесткого диска

Если копирование образа жесткого диска с установленным Агентом администрирования было выполнено без учета правил развертывания, часть устройств в Консоли администрирования может отображаться как один значок устройства, постоянно меняющий имя.

Можно использовать следующие способы решения этой проблемы:

- Удаление Агента администрирования.

  Этот способ является самым надежным. На устройствах, которые были скопированы из образа неправильно, нужно при помощи сторонних средств удалить Агент администрирования, а затем установить его заново. Удаление Агента администрирования не может быть выполнено средствами Kaspersky Security Center, поскольку для Сервера администрирования все проблемные устройства неразличимы (им всем соответствует один и тот же значок в Консоли администрирования).

- Запуск утилиты klmover с ключом "-dupfix".

  На проблемных устройствах (на всех, которые были скопированы из образа неправильно) необходимо при помощи сторонних средств однократно запустить утилиту klmover с ключом "-dupfix" (klmover -dupfix), расположенную в папке установки Агента администрирования. Запуск утилиты не может быть выполнен средствами Kaspersky Security Center, поскольку для Сервера администрирования все проблемные устройства неразличимы (им всем соответствует один и тот же значок в Консоли администрирования).

  Затем следует удалить значок, на который отображались проблемные устройства до запуска утилиты.

- Ужесточение правила обнаружения неправильно скопированных устройств.

Этот способ можно использовать только в случае, если установлены Сервер администрирования и Агенты администрирования версии 10 Service Pack 1 или новее.

Следует ужесточить правило обнаружения неправильно скопированных Агентов администрирования таким образом, чтобы изменение NetBIOS-имени устройства приводило к автоматической "починке" таких Агентов администрирования (предполагается, что скопированные устройства имеют различные NetBIOS-имена).

На устройстве с Сервером администрирования нужно импортировать в Реестр представленный ниже reg-файл и перезапустить службу Сервера администрирования.

- Если на устройстве с Сервером администрирования установлена 32-разрядная операционная система:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

- Если на устройстве с Сервером администрирования установлена 64-разрядная операционная система:

```
REGEDIT4
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
"KLSRV_CheckClones"=dword:00000003
```

Развертывание с помощью механизма групповых политик Microsoft Windows

Первоначальное развертывание Агентов администрирования рекомендуется осуществлять с помощью групповых политик Microsoft Windows при выполнении следующих условий:

- устройства являются членами домена Active Directory;
- план развертывания позволяет дождаться штатной перезагрузки устройств до начала развертывания на них Агентов администрирования, или к устройствам можно принудительно применить групповую политику Windows.

Суть этого способа развертывания заключается в следующем:

- Дистрибутив приложения в формате Microsoft Installer (MSI-пакет) размещается в папке общего доступа (в папке, к которой имеют доступ на чтение учетные записи LocalSystem устройств).
- В групповой политике Active Directory создается объект установки данного дистрибутива.
- Область действия установки задается привязкой к организационному подразделению и / или к группе безопасности, в которую входят устройства.
- При очередном входе устройства в домен (до входа в систему пользователей устройства) выполняется проверка наличия требуемого приложения среди установленных приложений. Если приложение отсутствует, происходит загрузка дистрибутива с заданного в политике ресурса и его установка.

Одним из преимуществ этого способа развертывания является то, что назначенные приложения устанавливаются на устройства при загрузке операционной системы еще до входа пользователя в систему. Даже если пользователь, имеющий необходимые права, удалит приложение, при следующей загрузке операционной системы оно будет установлено снова. Недостатком этого способа развертывания является то, что произведенные администратором изменения в групповой политике не вступят в силу до перезагрузки устройств (без применения дополнительных средств).

С помощью групповых политик можно устанавливать как Агент администрирования, так и другие приложения, инсталляторы которых имеют формат Windows Installer.

При выборе этого способа развертывания, помимо прочего, необходимо оценить нагрузку на файловый ресурс, с которого будет осуществляться копирование файлов на устройства при применении групповой политики Windows.

Работа с политиками Microsoft Windows с помощью задачи удаленной установки приложений Kaspersky Security Center

Самым простым способом установки приложений с помощью групповых политик Microsoft Windows является выбор параметра **Назначить установку инсталляционного пакета в групповых политиках Active Directory** в свойствах задачи удаленной установки приложений Kaspersky Security Center. В этом случае при запуске задачи Сервер администрирования самостоятельно выполнит следующие действия:

- Создаст необходимые объекты в групповой политике Microsoft Windows.
- Создаст специальные группы безопасности, в которые включит устройства, и назначит установку выбранных приложений для этих групп безопасности. Состав групп безопасности будет актуализироваться при каждом запуске задачи в соответствии с набором устройств на момент запуска.

Для обеспечения работоспособности данной функции следует указать в параметрах задачи учетную запись, имеющую права на редактирование групповых политик Active Directory.

Если с помощью одной задачи предполагается установить и Агент администрирования, и другое приложение, выбор параметра **Назначить установку инсталляционного пакета в групповых политиках Active Directory** приведет к созданию в политике Active Directory объекта установки только для Агента администрирования. Второе выбранное в задаче приложение будет устанавливаться уже средствами Агента администрирования, как только он будет установлен на устройстве. Если по какой-то причине необходимо установить отличное от Агента администрирования приложение именно с помощью групповых политик Windows, то нужно создать задачу установки только для этого инсталляционного пакета (без пакета Агента администрирования). Не все приложения могут быть установлены с помощью групповых политик Microsoft Windows. О такой возможности вы можете узнать, обратившись к информации о способах установки приложения.

В случае, когда необходимые объекты создаются в групповой политике средствами Kaspersky Security Center, в качестве источника инсталляционного пакета будет использована папка общего доступа Kaspersky Security Center. При планировании развертывания следует соотнести скорость чтения из этой папки с количеством устройств и размером устанавливаемого дистрибутива. Возможно, будет целесообразно расположить папку общего доступа Kaspersky Security Center в мощном специализированном файловом хранилище.

Помимо простоты, автоматическое создание групповых политик Windows средствами Kaspersky Security Center имеет еще одно преимущество: при планировании установки Агента администрирования легко указать группу администрирования Kaspersky Security Center, в которую будут автоматически перемещаться устройства по завершении установки. Группу можно указать в мастере создания задачи или в окне параметров задачи удаленной установки.

При работе с групповыми политиками Windows средствами Kaspersky Security Center задание устройств для объекта групповой политики осуществляется путем создания группы безопасности. Kaspersky Security Center синхронизирует состав группы безопасности с текущим набором устройств задачи. При использовании иных средств для работы с групповыми политиками можно привязывать объекты групповых политик непосредственно к выбранным подразделениям Active Directory.

Самостоятельная установка приложений с помощью политик Microsoft Windows

Администратор может самостоятельно создать в групповой политике Windows объекты, необходимые для установки. В этом случае можно сослаться на пакеты, лежащие в папке общего доступа Kaspersky Security Center, или выложить пакеты на отдельный файловый сервер и сослаться на них.

Возможны следующие сценарии установки:

- Администратор создает инсталляционный пакет и настраивает его свойства в Консоли администрирования. Объект групповой политики ссылается на MSI-файл этого сконфигурированного пакета, лежащего в папке общего доступа Kaspersky Security Center.

- Администратор создает инсталляционный пакет и настраивает его свойства в Консоли администрирования. Затем администратор копирует целиком подпапку EXEC этого пакета из папки общего доступа Kaspersky Security Center в папку на специализированном файловом ресурсе организации. Объект групповой политики ссылается MSI-файл этого пакета, лежащего в подпапке на специализированном файловом ресурсе организации.

- Администратор загружает дистрибутив приложения (в том числе дистрибутив Агента администрирования) из интернета и выкладывает его на специализированный файловый ресурс организации. Объект групповой политики ссылается MSI-файл этого пакета, лежащего в подпапке на специализированном файловом ресурсе организации. Настройка параметров инсталляции осуществляется путем настройки свойств MSI или настройкой файлов трансформации MST.

Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center

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 при условии, что на каждом устройстве есть учетные записи пользователей с правами локального администратора.

Принудительная установка может быть использована и в случае, если устройства не доступны Серверу администрирования непосредственно: например, устройства расположены в изолированных сетях, или устройства расположены в локальной сети, а Сервер администрирования – в демилитаризованной зоне.

В случае первоначального развертывания Агент администрирования не устанавливается. Поэтому в параметрах задачи удаленной установки невозможно выбрать распространение файлов, необходимых для установки приложения с помощью Агента администрирования. Вы можете распространять файлы, только используя ресурсы операционной системы с помощью Сервера администрирования или точек распространения.

Служба Сервера администрирования должна запускаться под учетной записью, имеющей права администратора на целевых устройствах. Также вы можете указать учетную запись, имеющую доступ к административным ресурсам общего доступа admin$, в параметрах задачи удаленной установки.

По умолчанию задача удаленной установки применяется к устройствам и использует учетные данные учетной записи, под которой запущен Сервер администрирования. Обратите внимание, что это учетная запись, используемая для доступа к административным ресурсам общего доступа admin$, а не учетная запись, под которой выполняется задача удаленной установки. Установка выполняется под учетной записью LocalSystem.

Вы можете указать целевые устройства явно (списком), выбрав группу администрирования Kaspersky Security Center, 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 сервисов. Рассылка инсталляционных пакетов на целевые устройства выполняется с помощью функции Kaspersky Security Center, отвечающей за сетевое взаимодействие. При этом должны выполняться следующие условия:

- Целевые устройства доступны со стороны Сервера администрирования или со стороны точки распространения.
- В сети корректно работает разрешение имен для устройств.
- На целевых устройствах включены административные ресурсы общего доступа admin$.
- На целевых устройствах запущены следующие системные службы:
  - Сервер (LanmanServer).

    По умолчанию эта служба запущена.
  - DCOM Server Process Launcher (DcomLaunch).
  - RPC Endpoint Mapper (RpcEptMapper).
  - Вызов удаленной процедуры (Remote Procedure Call, RpcSs).
- TCP-порт 445 открыт на целевых устройствах для обеспечения удаленного доступа с помощью инструментария управления Windows (WMI).

  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 Сервера администрирования и точек распространения с целевыми устройствами.
- В параметрах безопасности политики домена Active Directory разрешено обеспечивать работу NTLM-протокола при развертывании Агента администрирования.

- На целевых устройствах под управлением Microsoft Windows XP режим Simple File Sharing выключен.
- На целевых устройствах настроена модель совместного доступа и безопасности *Классическая – локальные пользователи выполняют аутентификацию самих себя*. Такая модель не может быть *Только гостевой – локальные пользователи выполняют аутентификацию как Гость*.
- Устройства являются членами домена, либо на устройствах заблаговременно созданы унифицированные учетные записи с административными правами.

Чтобы успешно развернуть Агент администрирования или другие приложения на устройстве, не подключенном к домену Active Directory с версией операционной системы Windows Server 2003 и выше, необходимо выключить удаленный UAC на этом устройстве. Удаленный UAC – это одна из причин, по которой учетные записи локальных администраторов не могут получить доступ к admin$, который требуется для принудительного развертывания Агента администрирования и других приложений. Выключение удаленного UAC не влияет на локальный UAC.

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

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

Упрощенным способом создания задач для принудительной установки приложений является автоматическая установка. Для этого в свойствах группы администрирования вам нужно открыть список инсталляционных пакетов и выбрать те пакеты, которые должны быть установлены на устройствах этой группы. В результате на всех устройствах этой группы и ее подгрупп будут автоматически установлены выбранные инсталляционные пакеты. Период, в течение которого будут установлены пакеты, зависит от пропускной способности сети и общего количества устройств в сети.

Чтобы снизить нагрузку на Сервер администрирования при распространении инсталляционных пакетов на целевые устройства, вы можете выбрать установку с помощью точек распространения в задаче установки. Следует учитывать, что данный способ установки создает значительную нагрузку на устройства, назначенные точками распространения. Рекомендуется выбирать устройства, соответствующие требованиям для точек распространения. Если вы используете точки распространения, вам нужно убедиться, что они присутствуют в каждой из изолированных подсетей, на которых размещены целевые устройства.

Использование точек распространения в качестве локальных центров установки может быть удобно и для установки на устройства в подсетях, соединенных с Сервером администрирования узким каналом связи при наличии широкого канала связи между устройствами внутри подсети.

Объем свободного места в разделе с папкой %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit должен многократно превосходить суммарный объем дистрибутивов устанавливаемых приложений.

Запуск автономных пакетов, сформированных Kaspersky Security Center

Описанные выше способы первоначального развертывания Агента администрирования и приложений могут быть реализованы не всегда из-за невозможности выполнить все необходимые условия. В таких случаях из подготовленных администратором инсталляционных пакетов с необходимыми параметрами установки средствами Kaspersky Security Center можно создать единый исполняемый файл, который называется *автономным пакетом установки*. Автономный инсталляционный пакет размещается в папке общего доступа Kaspersky Security Center.

При помощи Kaspersky Security Center можно разослать по электронной почте выбранным пользователям ссылку на этот файл в папке общего доступа с просьбой запустить файл (интерактивно или с ключом тихой установки "-s"). Автономный инсталляционный пакет можно прикрепить к сообщению электронной почты для пользователей устройств, не имеющих доступа к папке общего доступа Kaspersky Security Center. Администратор может скопировать автономный пакет на съемный диск и доставить пакет на нужное устройство с целью его последующего запуска.

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

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

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

Автономный инсталляционный пакет Агент администрирования для Linux имеет дополнительную зависимость от утилиты nmap. Если утилита nmap отсутствует или имеет версию ниже 6.0, функциональность Broadcast DHCP Discover не поддерживается.

Возможности ручной установки приложений

Администраторы или опытные пользователи могут устанавливать приложения вручную в интерактивном режиме. При этом можно использовать как исходные дистрибутивы, так и сформированные из них инсталляционные пакеты, расположенные в папке общего доступа Kaspersky Security Center. Инсталляторы по умолчанию работают в интерактивном режиме, запрашивая у пользователя все необходимые значения параметров. Но при запуске процесса setup.exe из корня инсталляционного пакета с ключом "-s" инсталлятор будет работать в тихом режиме с параметрами, заданными при настройке инсталляционного пакета.

При запуске setup.exe из корня инсталляционного пакета расположенного в папке общего доступа Kaspersky Security Center, сначала произойдет копирование пакета во временную локальную папку, затем из локальной папки будет запущен инсталлятор приложения.

Создание MST-файла

Чтобы преобразовать содержимое пакета MSI и применить пользовательские параметры к существующему файлу MSI, необходимо создать файл преобразования в формате MST. Для этого используйте редактор Orca.exe, входящий в состав Windows SDK.

Чтобы создать MST-файл:

1. Запустите редактор Orca.exe.
2. Перейдите на вкладку **File** и в меню нажмите **Open**.
3. Выберите файл Kaspersky Network Agent.msi.
4. Перейдите на вкладку **Transformation** и в меню выберите **New transformation**.
5. В столбце **Таблицы** выберите **Свойство** и укажите следующие значения:
   - *EULA=1*
   - *SERVERADDRESS=<Адрес Сервера администрирования>*

   Нажмите на кнопку **Сохранить**.
6. Перейдите на вкладку **Transform** и в меню выберите **Generate Transform**.
7. В открывшемся окне укажите имя создаваемого файла трансформации и нажмите на кнопку **Сохранить**.

MST-файл сохранен.

Удаленная установка приложений на устройства с установленным Агентом администрирования

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

Эта функция включается параметром **С помощью Агента администрирования** в свойствах задачи удаленной установки приложений.

Если параметр выбран, то передача на устройства инсталляционных пакетов с заданными администратором инсталляционными параметрами осуществляется по каналам связи между Агентом администрирования и Сервером администрирования.

Для оптимизации нагрузки на Сервер администрирования и минимизации трафика между Сервером администрирования и устройствами целесообразно назначать в каждой удаленной сети или в каждом широковещательном домене точки распространения (см. разделы "О точках распространения" и "Построение структуры групп администрирования и назначение точек распространения"). В этом случае распространение инсталляционных пакетов и параметров инсталлятора осуществляется с Сервера администрирования на устройства через точки распространения.

Также с использованием точек распространения можно выполнять широковещательную (многоадресную) рассылку инсталляционных пакетов, что позволяет многократно снизить сетевой трафик в ходе развертывания приложений.

При передаче инсталляционных пакетов на устройства по каналам связи между Агентами администрирования и Сервером администрирования подготовленные к передаче инсталляционные пакеты дополнительно кешируются в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. При использовании большого числа различных инсталляционных пакетов большого размера и при большом количестве точек распространения размер этой папки может существенно увеличиваться.

Удалять файлы из папки FTServer вручную невозможно. При удалении исходных инсталляционных пакетов соответствующие данные будут автоматически удаляться и из папки FTServer.

Данные, принимаемые точками распространения, сохраняются в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp.

Удалять файлы из папки $FTCITmp вручную невозможно. По мере завершения задач, использующих данные из папки, содержимое этой папки будет удаляться автоматически.

Поскольку инсталляционные пакеты распространяются по каналам связи между Сервером администрирования и Агентами администрирования из промежуточного хранилища в оптимизированном для передачи по сети формате, невозможно вносить изменения в инсталляционные пакеты в исходной папке инсталляционного пакета. Такие изменения не будут автоматически учтены Сервером администрирования. Если необходимо изменить вручную файлы инсталляционных пакетов (хотя делать это не рекомендуется), нужно обязательно изменить какие-либо параметры инсталляционного пакета в Консоли администрирования. Изменение параметров инсталляционного пакета в Консоли администрирования заставит Сервер администрирования обновить образ пакета в кеше, подготовленном для передачи на устройства.

Управление перезагрузкой устройств в задаче удаленной установки

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

Если используется задача удаленной установки приложений Kaspersky Security Center, в мастере создания задачи или в окне свойств созданной задачи (раздел **Перезагрузка операционной системы**) можно выбрать вариант действия при необходимости перезагрузки:

- **Не перезагружать устройство**. В этом случае автоматическая перезагрузка не будет выполнена. Для завершения установки потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки будет сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач установки на серверы и другие устройства, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**. В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения установки. Этот вариант подходит для задач установки на устройства, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**. На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Вариант **Запрашивать у пользователя** наиболее подходит для рабочих станций, пользователи которых должны иметь возможность выбрать наиболее подходящий момент для перезагрузки.

Целесообразность обновления баз в инсталляционном пакете приложения безопасности

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

Использование средств удаленной установки приложений Kaspersky Security Center для запуска на управляемых устройствах произвольных исполняемых файлов

С помощью мастера создания инсталляционного пакета можно выбрать произвольный исполняемый файл и задать для него параметры командной строки. При этом в инсталляционный пакет можно поместить как сам выбранный файл, так и всю папку, в которой этот файл содержится. Затем следует создать задачу удаленной установки и выбрать созданный инсталляционный пакет.

В ходе работы задачи на устройствах будет запущен указанный при создании исполняемый файл с заданными параметрами командной строки.

Если используются инсталляторы в формате Microsoft Windows Installer (MSI), Kaspersky Security Center использует штатные возможности по анализу результата установки.

Если есть лицензия на Системное администрирование, при создании инсталляционного пакета для одного из поддерживаемых приложений, распространенных в корпоративной среде, Kaspersky Security Center также использует правила установки и анализа результатов установки, имеющиеся в его обновляемой базе.

В иных случаях для исполняемых файлов задача по умолчанию дожидается завершения запущенного процесса и всех порожденных им дочерних процессов. По завершении запущенных процессов задача будет завершена успешно независимо от кода возврата исходного процесса. Чтобы изменить такое поведение задачи, перед созданием задачи следует изменить вручную файлы с расширением .kpd, сформированные Kaspersky Security Center в папке созданного инсталляционного пакета и в его подпапках.

Файлы с расширением kpd используют кодировку ASCII. Файлы с расширением kud используют кодировку Юникод.

Для того чтобы задача не ожидала завершения запущенного процесса, в секции [SetupProcessResult] нужно задать значение 0 для параметра Wait:

```
[SetupProcessResult]
Wait=0
```

Для того чтобы на платформе Windows задача ожидала только завершения исходного процесса, но не порожденных им дочерних процессов, нужно в секции [SetupProcessResult] задать значение 0 для параметра WaitJob, например:

```
[SetupProcessResult]
WaitJob=0
```

Для того чтобы задача завершалась успешно или с ошибкой в зависимости от кода возврата запущенного процесса, создайте исполняемый файл с расширением bat, который сохранит код ошибки в файл, например:

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

Затем измените файлы с расширением kud, сформированные Kaspersky Security Center в папке созданного инсталляционного пакета:

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=Installation completed successfully.
[SetupMainResult_ErrorCodes]
1=Installation script error
2=Custom error
```

В этом случае любой код, отличный от перечисленных, будет означать ошибку.

Для того чтобы в результатах задачи отображалась строка с комментарием об успешном завершении задачи или сообщения об ошибках, нужно задать краткие описания ошибок, соответствующих кодам возврата процесса, в секциях [SetupProcessResult_SuccessCodes] и [SetupProcessResult_ErrorCodes], например:

```
[SetupProcessResult_SuccessCodes]
0= Installation completed successfully
3010=A reboot is required to complete the installation
[SetupProcessResult_ErrorCodes]
1602=Installation cancelled by the user
1603=Fatal error during installation
```

Для того чтобы задействовать средства Kaspersky Security Center по управлению перезагрузкой устройства (если перезагрузка необходима для завершения операции), нужно дополнительно перечислить коды возврата процесса, означающие необходимость перезагрузки, в секции [SetupProcessResult_NeedReboot]:

```
[SetupProcessResult_NeedReboot]
3010=
```

Мониторинг развертывания

Для контроля развертывания Kaspersky Security Center, а также для контроля наличия на управляемых устройствах приложения безопасности и Агента администрирования, следует обращать внимание на цветовой индикатор в блоке **Развертывание**. Индикатор расположен в рабочей области узла Сервер администрирования в главном окне Консоли администрирования. Индикатор отображает текущее состояние развертывания. Рядом с индикатором отображается количество устройств с установленными Агентами администрирования и приложениями безопасности. При наличии активных задач установки отображается прогресс выполнения задач. При наличии ошибок установки, здесь отображается количество ошибок. Просмотреть детальную информацию об ошибке можно по ссылке.

Также можно воспользоваться диаграммой развертывания в рабочей области папки **Управляемые устройства** на вкладке **Группы**. Диаграмма отражает процесс развертывания: количество устройств без Агента администрирования, с Агентом администрирования, с Агентом администрирования и приложением безопасности.

Более детальное описание хода развертывания (или работы конкретной задачи установки) можно увидеть в окне результатов выполнения соответствующей задачи удаленной установки: В контекстном меню задачи выберите **Результаты**. В окне отображаются два списка: в верхнем списке содержится список состояний задачи на устройствах, а в нижнем – список событий задачи на устройстве, которое в данный момент выбрано в верхнем списке.

Информация об ошибках при развертывании записывается в журнал событий Kaspersky Event Log Сервера администрирования. Информация об ошибках также доступна в соответствующей выборке событий в узле Сервера администрирования на вкладке **События**.

Настройка параметров инсталляторов

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

Общая информация

Инсталляторы компонентов Kaspersky Security Center 15.1 – Сервера администрирования, Агента администрирования, Консоли администрирования – построены на технологии Windows Installer. Ядром инсталлятора является MSI-пакет. Этот формат упаковки дистрибутива позволяет использовать все преимущества технологии Windows Installer: масштабируемость, возможность использовать систему патчевания, систему трансформации, возможность установки централизованно сторонними решениями, прозрачность регистрации в операционной системе.

Установка в тихом режиме (с файлом ответов)

В инсталляторах Сервера администрирования и Агента администрирования реализована возможность работы с файлом ответов (ss_install.xml), в котором записаны параметры для установки в тихом режиме без участия пользователя. Файл ss_install.xml расположен в той же папке, что и MSI-пакет, и используется автоматически при установке в тихом режиме. Вы можете включить режим автоматической установки с помощью ключа командной строки "/s".

Пример запуска:

```
setup.exe /s
```

Прежде чем запускать приложение установки в тихом режиме, прочтите Лицензионное соглашение. Если в состав дистрибутива Kaspersky Security Center не входит TXT файл с текстом Лицензионного соглашения, вы можете загрузить этот файл с сайта "Лаборатории Касперского".

Файл ss_install.xml представляет собой внутренний формат параметров инсталлятора Kaspersky Security Center. В составе дистрибутивов поставляется файл ss_install.xml с параметрами по умолчанию.

Не следует изменять файл ss_install.xml вручную. Этот файл изменяется средствами Kaspersky Security Center при изменении параметров инсталляционных пакетов в Консоли администрирования.

Чтобы изменить файл ответов для установки Сервера администрирования:

1. Откройте дистрибутив Kaspersky Security Center. Если вы используете полный пакет EXE-файла, распакуйте его.
2. Сформируйте папку Сервер, откройте командную строку и выполните следующую команду:

   ```
   setup.exe /r ss_install.xml
   ```

   Запустится приложение установки Kaspersky Security Center.
3. Следуйте инструкциям мастера, чтобы настроить установку Kaspersky Security Center.

   По завершении работы мастера файл ответов автоматически изменится в соответствии с новыми параметрами, указанными вами.

Установка Агента администрирования в тихом режиме (без файла ответов)

Агент администрирования можно установить при помощи одного только msi-пакета, задавая при этом значения свойств MSI стандартным образом. Такой сценарий позволяет устанавливать Агент администрирования, используя групповые политики.

Не переименовывайте инсталляционный пакет Kaspersky Network Agent.msi. Переименование пакета может привести к ошибкам установки при обновлении Агента администрирования.

Для того чтобы не возникал конфликт между параметрами, заданными с помощью свойств MSI, и параметрами, заданными в файле ответов, предусмотрена возможность отключения файла ответов путем задания свойства `DONT_USE_ANSWER_FILE=1`. MSI-файл расположен в дистрибутиве приложения Kaspersky Security Center в папке Packages\NetAgent\exec. Ниже приведен пример запуска инсталлятора Агента администрирования с помощью msi-пакета.

Установка Агента администрирования в неинтерактивном режиме требует принятия Лицензионного соглашения. Используйте параметр `EULA=1`, только если вы полностью прочитали, понимаете и принимаете условия Лицензионного соглашения.

Пример:
```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

Также параметры инсталляции msi-пакета можно задать, подготовив предварительно файл трансформации (файл с расширением mst). Команда будет выглядеть следующим образом:

Пример:
```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

В одной команде можно указать более одного файла трансформации.

Если вы хотите обновить Агент администрирования с помощью установщика Windows Installer, выполните следующую команду:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Частичная настройка параметров установки через setup.exe

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

Команда будет выглядеть следующим образом:

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

Параметры установки Сервера администрирования

В таблице ниже описаны свойства MSI, которые можно настраивать при установке Сервера администрирования. Все параметры являются необязательными, кроме EULA и PRIVACYPOLICY.

Свойство MSI	Описание	Доступные значения
EULA	Согласие с условиями Лицензионного соглашения (обязательный параметр).	• 1 – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения настоящего Лицензионного соглашения. • Другое значение или не задано – не согласны с условиями Лицензионного соглашения (установка не выполняется).
PRIVACYPOLICY	Согласие с условиями Политики конфиденциальности (обязательный параметр).	• 1 – Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности. Я подтверждаю, что полностью прочитал(а) и понимаю Политику конфиденциальности. • Другое значение или не задано – Я не принимаю условия Политики конфиденциальности (установка не выполняется).
INSTALLATIONMODETYPE	Тип установки Сервера администрирования.	• Стандартная. • Выборочная.
INSTALLDIR	Папка установки приложения.	Строковое значение.
ADDLOCAL	Список компонентов для установки (через запятую).	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Минимальный достаточный для корректной установки Сервера администрирования список компонентов: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Размер сети.	• NRT_1_100 – от 1 до 100 устройств. • NRT_100_1000 – от 101 до 1000 устройств. • NRT_GREATER_1000 – более 1000 устройств.
SRV_ACCOUNT_TYPE	Способ задания пользователя для работы службы Сервера администрирования.	• SrvAccountDefault – учетная запись пользователя будет создана автоматически. • SrvAccountUser – учетная запись пользователя задана вручную.
SERVERACCOUNTNAME	Имя пользователя для службы.	Строковое значение.
SERVERACCOUNTPWD	Пароль пользователя для службы.	Строковое значение.
DBTYPE	Тип базы данных.	• MySQL – будет использоваться база данных MySQL или MariaDB. • MSSQL – будет использоваться база данных Microsoft SQL Server (SQL Express).
MYSQLSERVERNAME	Полное имя сервера MySQL или MariaDB.	Строковое значение.
MYSQLSERVERPORT	Номер порта для подключения к серверу MySQL или MariaDB.	Числовое значение.
MYSQLDBNAME	Имя базы данных сервера MySQL или MariaDB.	Строковое значение.
MYSQLACCOUNTNAME	Имя пользователя для подключения к базе сервера MySQL или MariaDB.	Строковое значение.
MYSQLACCOUNTPWD	Пароль пользователя для подключения к базе сервера MySQL или MariaDB.	Строковое значение.
MSSQLCONNECTIONTYPE	Тип использования базы данных MSSQL.	• InstallMSSEE – установить из пакета. • ChooseExisting – использовать установленный сервер.
MSSQLSERVERNAME	Полное имя экземпляра SQL Server.	Строковое значение.
MSSQLDBNAME	Имя базы данных SQL Server.	Строковое значение.
MSSQLAUTHTYPE	Способ аутентификации при подключении к SQL Server.	• Windows. • SQLServer.
MSSQLACCOUNTNAME	Имя пользователя для подключения к SQL Server в режиме SQLServer.	Строковое значение.

Свойство MSI	Описание	Доступные значения
MSSQLACCOUNTPWD	Пароль пользователя для подключения к SQL Server в режиме SQLServer.	Строковое значение.

CREATE_SHARE_TYPE	Способ задания папки общего доступа.	• Create – создать новую папку общего доступа. В этом случае должны быть заданы следующие свойства:
		  • SHARELOCALPATH – путь к локальной папке.
		  • SHAREFOLDERNAME – сетевое имя папки.
		• Пусто – должно быть задано свойство EXISTSHAREFOLDERNAME.

EXISTSHAREFOLDERNAME	Полный путь к существующей папке общего доступа.	Строковое значение.
SERVERPORT	Номер порта для подключения к Серверу администрирования.	Числовое значение.
SERVERSSLPORT	Номер порта для установки SSL-соединения с Сервером администрирования.	Числовое значение.
SERVERADDRESS	Адрес Сервера администрирования.	Строковое значение.
SERVERCERT2048BITS	Длина ключа для сертификата Сервера администрирования (в битах).	• 1 – длина ключа для сертификата Сервера администрирования составляет 2048 бит. • 0 – длина ключа для сертификата Сервера администрирования составляет 1024 бит. • Если параметр не задан, длина ключа для сертификата Сервера администрирования составляет 2048 бит.
MOBILESERVERADDRESS	Адрес Сервера администрирования для подключения мобильных устройств; игнорируется, если не выбран компонент MobileSupport.	Строковое значение.

Параметры установки Агента администрирования

В таблице ниже описаны свойства MSI, которые можно настраивать при установке Агента администрирования. Все параметры являются необязательными, кроме EULA и SERVERADDRESS.

Параметры установки Агента администрирования в тихом режиме

Свойство MSI	Описание	Доступные значения
EULA	Согласие с условиями Лицензионного соглашения	• 1 – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения настоящего Лицензионного соглашения. • 0 – Я не принимаю условия Лицензионного соглашения (установка не выполняется). • Значение не задано – Я не принимаю условия Лицензионного соглашения (установка не выполняется).
DONT_USE_ANSWER_FILE	Читать параметры установки из файла ответов.	• 1 – Не использовать. • другое значение или не задано – читать.
INSTALLDIR	Путь к папке установки Агента администрирования.	Строковое значение.
SERVERADDRESS	Адрес Сервера администрирования (обязательный параметр).	Строковое значение.
SERVERPORT	Номер порта подключения к Серверу администрирования.	Числовое значение.

Свойство MSI	Описание	Доступные значения
SERVERSSLPORT	Номер порта для защищенного подключения к Серверу администрирования с использованием протокола SSL.	Числовое значение.
USESSL	Использовать ли SSL-соединение.	• 1 – использовать; • другое значение или не задано – не использовать.
OPENUDPPORT	Открыть ли UDP-порт.	• 1 – открывать; • другое значение или не задано – не открывать.
UDPPORT	Номер UDP-порта.	Числовое значение.
USEPROXY	Использовать ли прокси-сервер. В целях совместимости не рекомендуется указывать параметры подключения к прокси-серверу в параметрах инсталляционного пакета Агента администрирования.	• 1 – использовать; • другое значение или не задано – не использовать.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Адрес прокси-сервера и номер порта для подключения к прокси-серверу.	Строковое значение.
PROXYLOGIN	Учетная запись для подключения к прокси-серверу.	Строковое значение.
PROXYPASSWORD	Пароль учетной записи для подключения к прокси-серверу (Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.)	Строковое значение.
GATEWAYMODE	Режим использования шлюза соединения.	• 0 – не использовать шлюз соединений; • 1 – использовать данный Агент администрирования в качестве шлюза соединений; • 2 – подключаться к Серверу администрирования через шлюз соединений.
GATEWAYADDRESS	Адрес шлюза соединений.	Строковое значение.
CERTSELECTION	Способ получения сертификата.	• GetOnFirstConnection – получить сертификат от Сервера администрирования; • GetExistent – задать существующий сертификат. Если выбран этот вариант, должно быть задано свойство CERTFILE.
CERTFILE	Путь к файлу сертификата.	Строковое значение.
VMVDI	Включить динамический режим для VDI.	• 1 – включать; • 0 – не включать; • Значение не задано – не включать.
VMOPTIMIZE	Являются ли параметры Агента администрирования оптимальными для гипервизора.	• 1 – включать; • 0 – не включать; • Значение не задано – не включать.
LAUNCHPROGRAM	Запускать ли службу Агента администрирования после установки. Параметр игнорируется, если VMVDI=1.	• 1 – запускать; • другое значение или не задано – не запускать.
NAGENTTAGS	Тег для Агента администрирования (имеет приоритет над тегом, указанным в файле ответов).	Строковое значение.

Виртуальная инфраструктура

Kaspersky Security Center поддерживает работу с виртуальными машинами. Вы можете установить Агент администрирования и приложения безопасности на каждую виртуальную машину, а также вы можете защищать виртуальные машины на уровне гипервизора. В первом случае для защиты виртуальных машин можно использовать как обычное приложение безопасности, так и Kaspersky Security для виртуальных сред Легкий агент. Во втором случае вы можете использовать Kaspersky Security для виртуальных сред Защита без агента.

Kaspersky Security Center поддерживает откат виртуальных машин к предыдущему состоянию.

Рекомендации по снижению нагрузки на виртуальные машины

В случае инсталляции Агента администрирования на виртуальную машину следует рассмотреть возможность отключения той части функциональности Kaspersky Security Center, которая не очень полезна для виртуальных машин.

При установке Агента администрирования на виртуальную машину или на шаблон, из которого в дальнейшем будут получены виртуальные машины, рекомендуется выполнить следующие действия:

- если выполняется удаленная установка, в окне свойств инсталляционного пакета Агента администрирования (в разделе **Дополнительно**) выбрать параметр **Оптимизировать параметры для VDI**;
- если выполняется интерактивная установка с помощью мастера, в окне мастера выбрать параметр **Оптимизировать параметры Агента администрирования для виртуальной инфраструктуры**.

Выбор параметров изменит параметры Агента администрирования таким образом, чтобы по умолчанию (до применения политики) были выключены следующие функции:

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

Как правило, перечисленные функции не нужны на виртуальных машинах в силу того, что программное обеспечение и виртуальное аппаратное обеспечение на них единообразны.

Выключение функций обратимо. Если любая из выключенных функций все же нужна, ее можно включить при помощи политики Агента администрирования, или в локальных параметрах Агента администрирования. Локальные параметры Агента администрирования доступны из контекстного меню соответствующего устройства в Консоли администрирования.

Поддержка динамических виртуальных машин

Kaspersky Security Center поддерживает динамические виртуальные машины. Если в сети организации развернута виртуальная инфраструктура, то в некоторых случаях могут использоваться динамические (временные) виртуальные машины. Такие машины создаются с уникальными именами из заранее подготовленного администратором шаблона. Пользователь работает с созданной машиной некоторое время, а после выключения виртуальная машина удаляется из виртуальной инфраструктуры. Если в сети организации развернут Kaspersky Security Center, то виртуальная машина с установленным на ней Агентом администрирования добавляется в базу данных Сервера администрирования. После выключения виртуальной машины запись о ней должна быть также удалена и из базы данных Сервера администрирования.

Чтобы функциональность автоматического удаления записей о виртуальных машинах работала, при установке Агента администрирования на шаблон, из которого будут созданы динамические виртуальные машины, нужно выбрать параметр **Включить динамический режим для VDI**:

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

Параметр **Включить динамический режим для VDI** не следует выбирать при установке Агента администрирования на физические устройства.

Если нужно, чтобы события с динамических виртуальных машин сохранялись на Сервере администрирования некоторое время после удаления машин, то следует в окне свойств Сервера администрирования в разделе **Хранилище событий** выбрать параметр **Хранить события после удаления устройств** и указать максимальное время хранения событий в днях.

Не рекомендуется включать шифрование дисков на динамических виртуальных машинах.

Поддержка копирования виртуальных машин

Копирование виртуальной машины с установленным на нее Агентом администрирования или ее создание из шаблона с установленным Агентом администрирования эквивалентно развертыванию Агентов администрирования захватом и копированием образа жесткого диска. Поэтому в общем случае при копировании виртуальных машин нужно выполнять те же действия, что и при развертывании копированием образа диска.

Однако в описанных ниже двух случаях Агент администрирования обнаруживает факт копирования автоматически. Поэтому выполнять сложные действия, описанные в разделе "Развертывание захватом и копированием жесткого диска устройства", необязательно:

- При установке Агента администрирования был выбран параметр **Включить динамический режим для VDI**: после каждой перезагрузки операционной системы такая виртуальная машина будет считаться новым устройством, независимо от факта ее копирования.

- Используется один из следующих гипервизоров: VMware™, HyperV® или Xen®: Агент администрирования определит факт копирования виртуальной машины по изменившимся идентификаторам виртуального аппаратного обеспечения.

Анализ изменений виртуального аппаратного обеспечения не абсолютно надежен. Прежде чем широко использовать данный метод, следует предварительно проверить его работоспособность на небольшом количестве виртуальных машин для используемой в организации версии гипервизора.

Поддержка отката файловой системы для устройств с Агентом администрирования

Kaspersky Security Center является распределенным приложением. Откат файловой системы в предыдущее состояние на одном из устройств с установленным Агентом администрирования приведет к рассинхронизации данных и неправильной работе Kaspersky Security Center.

Откат файловой системы (или ее части) в предыдущее состояние может происходить в следующих случаях:

- при копировании образа жесткого диска;

- при восстановлении состояния виртуальной машины средствами виртуальной инфраструктуры;

- при восстановлении данных из резервной копии или точки восстановления.

Для Kaspersky Security Center критичны только те сценарии, при которых стороннее программное обеспечение на устройствах с установленным Агентом администрирования затрагивает папку %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\. Поэтому следует всегда исключать эту папку из процедуры восстановления, если это возможно.

Поскольку в ряде организаций регламент работы предполагает выполнение отката состояния файловой системы устройств, в Kaspersky Security Center, начиная с версии 10 Maintenance Release 1 (Сервер администрирования и Агенты администрирования должны быть версии 10 Maintenance Release 1 или выше), была добавлена поддержка обнаружения отката файловой системы на устройствах с установленным Агентом администрирования. В случае обнаружения такие устройства автоматически переподключаются к Серверу администрирования с полной очисткой и полной синхронизацией данных.

В Kaspersky Security Center 15.1 поддержка обнаружения отката файловой системы включена по умолчанию.

Следует при любой возможности избегать отката папки %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ на устройствах с установленным Агентом администрирования, так как полная повторная синхронизация данных требует большого количества ресурсов.

Для устройства с установленным Сервером администрирования откат состояния системы недопустим. Недопустимым также является откат в предыдущее состояние базы данных, используемой Сервером администрирования.

Восстановить состояние Сервера администрирования из резервной копии можно только при помощи штатной утилиты klbackup.

Локальная установка приложений

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

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

Чтобы установить приложения локально на выбранное клиентское устройство:

1. Установите на клиентское устройство Агент администрирования и настройте связь клиентского устройства с Сервером администрирования.

2. Установите на устройство необходимые приложения согласно описаниям, изложенным в Руководствах к этим приложениям.

3. Установите на рабочее место администратора плагин управления для каждого из установленных приложений.

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

Локальная установка Агента администрирования

Чтобы установить Агент администрирования на устройство локально:

1. На устройстве запустите файл setup.exe из дистрибутива, полученного через интернет. Дополнительную информацию см. в следующих разделах: Получение инсталляционного пакета Агента администрирования из комплекта поставки Kaspersky Security Center.

   Откроется окно с выбором приложений "Лаборатории Касперского" для установки.

2. В окне с выбором приложений по ссылке **Установить только Агент администрирования Kaspersky Security Center** запустите мастер установки Агента администрирования. Следуйте далее указаниям мастера.

   a. **Сервер администрирования**

      Порт

Указан незащищенный порт, используемый Сервером администрирования для приема подключений от Агентов администрирования.

По умолчанию номер порта – 14000.

SSL-порт

Указан SSL-порт, используемый Сервером администрирования для приема подключений от Агентов администрирования.

По умолчанию номер порта – 13000.

Использовать SSL для соединения с Сервером администрирования

Если этот параметр включен, подключение к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

По умолчанию параметр включен.

Разрешить Агенту администрирования открыть UDP-порт

Если этот параметр включен, приложение установки автоматически открывает порт, используемый Сервером администрирования для управления клиентским устройством и получения информации о нем.

По умолчанию параметр включен.

UDP-порт

Позволяет настроить порт, используемый Сервером администрирования для управления клиентским устройством и получения информации о нем.

По умолчанию номер порта – 15000.

b. **Конфигурация прокси-сервера**

Использовать прокси-сервер

Если этот параметр включен, 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.

Адрес

Порт

Учетная запись

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.

c. **Шлюз соединения**

Не использовать шлюз соединения

Использовать в качестве шлюза соединения в демилитаризованной зоне

Выберите этот параметр, чтобы использовать Агент администрирования в качестве шлюза соединения в демилитаризованной зоне (DMZ) для подключения к Серверу администрирования, связи с ним и сохранения данных в безопасности на Агенте администрирования, во время передачи данных.

Подключаться к Серверу администрирования через шлюз соединения

Выберите этот параметр и укажите устройство, которое будет выполнять роль шлюза соединения.

d. **Сертификат Сервера администрирования**

e. **Теги агента**

f. **Дополнительные параметры**

Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"

Рекомендуется оставить этот параметр включенным. Вы можете снять этот флажок, чтобы отключить автоматическое обновление и установку патчей для компонентов Kaspersky Security Center. Администратор может снова включить автоматическую установку позже с помощью политики.

По умолчанию параметр выключен.

Включить защиту службы Агента администрирования

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.

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 Агента администрирования Kaspersky Security Center для VDI. Выключить поиск уязвимостей и инвентаризацию приложений и оборудования. Вы можете изменить заданные параметры, используя политики Агента администрирования.

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.

g. **Запуск приложения**

По окончании работы мастера установки Агент администрирования будет установлен на устройстве.

Вы можете просмотреть свойства службы Агента администрирования Kaspersky Security Center, а также запускать, останавливать и контролировать активность Агента администрирования с помощью стандартных инструментов Microsoft Windows: Управление компьютером\Службы.

Установка Агента администрирования в тихом режиме

Агент администрирования может быть установлен в тихом режиме, то есть без интерактивного ввода параметров установки. Для тихой установки используется инсталляционный пакет (MSI) Агента администрирования. MSI-файл расположен в дистрибутиве приложения Kaspersky Security Center в папке Packages\NetAgent\exec.

Не переименовывайте инсталляционный пакет Kaspersky Network Agent.msi. Переименование пакета может привести к ошибкам установки при обновлении Агента администрирования.

Установка Агента администрирования из пакета MSI возможна только в тихом режиме. Интерактивная установка Агента из пакета MSI не поддерживается.

Чтобы установить Агент администрирования на локальном устройстве в тихом режиме:

1. Прочитайте Лицензионное соглашение. Используйте команду ниже, только если вы поняли и принимаете условия Лицензионного соглашения.
2. Выполните команду

   ```
   msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
   ```

   где `setup_parameters` – список параметров и их значений, отделенных друг от друга пробелом (`PROP1=PROP1VAL PROP2=PROP2VAL`).

   В список параметров вам нужно включить параметр `EULA=1`. В противном случае Агент администрирования не будет установлен.

Если вы используете стандартные параметры подключения для Kaspersky Security Center и Агента администрирования на удаленных устройствах, выполните команду:

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

`/l*vx` – ключ для записи в журнал событий. Журнал событий создается при установке Агента администрирования и сохраняется в папке C:\windows\temp\nag_inst.log.

Помимо nag_inst.log, приложение создает файл $klssinstlib.log, который содержит журнал событий установки. Этот файл хранится в папке %windir%\temp or %temp%. Для устранения неполадок вам или специалисту Службы технической поддержки "Лаборатории Касперского" могут потребоваться оба файла журнала – nag_inst.log и $klssinstlib.log.

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

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

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

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

Если вы хотите обновить Агент администрирования с помощью установщика Windows Installer, выполните следующую команду:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

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

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

Чтобы выполнить установку Агента администрирования для Linux в тихом режиме:

1. Подготовьте требуемое устройство с операционной системой Linux для удаленной установки. Загрузите и создайте пакет удаленной установки, используя пакет Агента администрирования .deb или .rpm, с помощью любой подходящей системы управления пакетами.

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

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

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

4. Создайте файл ответов (в формате TXT). Добавьте в файл ответов список переменных в формате VARIABLE_NAME=variable_value, каждая переменная находится на отдельной строке.

   Для правильного использования файла ответов вам нужно включить в него минимальный набор из трех обязательных переменных:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

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

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

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

Имя переменной	Обязательная	Описание	Возможные значения
KLNAGENT_SERVER	Да	Содержит имя Сервера администрирования, представленное как полное доменное имя (FQDN) или IP-адрес.	DNS-имя устройства или IP-адрес.
KLNAGENT_AUTOINSTALL	Да	Определяет, включен ли тихий режим установки.	1 – тихий режим включен; пользователю не предлагается никаких действий во время установки. Другое – тихий режим выключен; пользователю могут быть предложены действия во время установки.
EULA_ACCEPTED	Да	Определяет, принимает ли пользователь Лицензионное соглашение Агента администрирования; если переменная не указана это может быть истолковано как отклонение Лицензионного соглашения.	1 – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения настоящего Лицензионного соглашения. Другое значение или не задано – Я не согласен с условиями Лицензионного соглашения (установка не выполняется).
KLNAGENT_PROXY_USE	Нет	Определяет, будет ли соединение с Сервером администрирования использовать параметры прокси-сервера. По умолчанию указано значение 0.	1 – используются параметры прокси-сервера. Другое – параметра прокси-сервера не используются.
KLNAGENT_PROXY_ADDR	Нет	Определяет адрес прокси-сервера, используемого для соединения с Сервером администрирования.	DNS-имя устройства или IP-адрес.
KLNAGENT_PROXY_LOGIN	Нет	Определяет имя пользователя, используемое для входа на прокси-сервер.	Любое существующее имя пользователя.
KLNAGENT_PROXY_PASSWORD	Нет	Определяет пароль пользователя, используемый для входа на прокси-сервер.	Любой набор букв и цифр, разрешенных форматом пароля в операционной системе.

KLNAGENT_VM_VDI	Нет	Определяет, установлен ли Агент администрирования на образ для создания динамических виртуальных машин.	1 – Агент администрирования установлен на образ, который затем будет использован для создания динамических виртуальных машин. Другое – во время установки образ не используется.
KLNAGENT_VM_OPTIMIZE	Нет	Определяет, являются ли параметры Агента администрирования оптимальными для гипервизора.	1 – локальные параметры Агента администрирования по умолчанию изменены таким образом, что они позволяют оптимизировать использование на гипервизоре.
KLNAGENT_TAGS	Нет	Перечисляет теги, назначенные экземпляру Агента администрирования.	Один или несколько тегов, разделенных точкой с запятой.
KLNAGENT_UDP_PORT	Нет	Определяет UDP-порт, используемый Агентом администрирования. По умолчанию указано значение 15000.	Любой существующий номер порта.
KLNAGENT_PORT	Нет	Определяет порт (не TLS), используемый Агентом администрирования. По умолчанию указано значение 14000.	Любой существующий номер порта.
KLNAGENT_SSLPORT	Нет	Определяет TLS-порт, используемый Агентом администрирования. По умолчанию указано значение 13000.	Любой существующий номер порта.
KLNAGENT_USESSL	Нет	Определяет, используется ли безопасность транспортного уровня (TLS) для подключения.	1 (по умолчанию) – используется TLS. Другое – TLS не используется.
KLNAGENT_GW_MODE	Нет	Определяет, используется ли шлюз соединения.	1 (по умолчанию) – текущие параметры не изменяются (при первом вызове шлюз соединения не указывается). 2 – шлюз соединения не используется. 3 – используется шлюз соединения. KLNAGENT_GW_ADDRESS – обязательный параметр. 4 – экземпляр Агента администрирования используется в качестве шлюза соединения в демилитаризованной зоне (DMZ). Требуется сертификат Сервера.

KLNAGENT_GW_ADDRESS	Нет	Определяет адрес шлюза соединения. Значение применимо, только если KLNAGENT_GW_MODE=3.	DNS-имя устройства или IP-адрес.
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Нет	Позволяет запустить утилиту регистрации пользователя в качестве владельца устройства после установки Агента администрирования. Если выключено, то регистрация в качестве владельца устройства недоступна для пользователя.	1 – после установки Агента администрирования будет запущена утилита регистрации пользователя в качестве владельца устройства. Другое – выключено.

5. Запустите инсталляционный пакет Агент администрирования. Переменная среды KLAUTOANSWERS, указывающая путь к файлу ответов, передается в команде для установки. Выполните одну из следующих команд:

   - Чтобы установить Агент администрирования из RPM-пакета на устройство с 32-разрядной операционной системой, выполните команду:
     `sudo KLAUTOANSWERS=<путь к файлу ответов> yum install ./klnagent-<номер сборки>.i386.rpm`

   - Чтобы установить Агент администрирования из RPM-пакета на устройство с 64-разрядной операционной системой, выполните команду:
     `sudo KLAUTOANSWERS=<путь к файлу ответов> yum install ./klnagent64-<номер сборки>.x86_64.rpm`

   - Чтобы установить Агент администрирования из RPM-пакета на устройство архитектуры ARM с 64-разрядной операционной системой, выполните команду:
     `sudo KLAUTOANSWERS=<путь к файлу ответов> yum install ./klnagent64-<номер сборки>.aarch64.rpm`

   - Чтобы установить Агент администрирования из DEB-пакета на устройство с 32-разрядной операционной системой, выполните команду:
     `sudo KLAUTOANSWERS=<путь к файлу ответов> apt install ./klnagent_<номер сборки>_i386.deb`

   - Чтобы установить Агент администрирования из DEB-пакета на устройство с 64-разрядной операционной системой, выполните команду:
     `sudo KLAUTOANSWERS=<путь к файлу ответов> apt install ./klnagent64_<номер сборки>_amd64.deb`

   - Чтобы установить Агент администрирования из DEB-пакета на устройство архитектуры ARM с 64-разрядной операционной системой, выполните команду:
     `sudo KLAUTOANSWERS=<путь к файлу ответов> apt install ./klnagent64_<номер сборки>_arm64.deb`

   В зависимости от конфигурации операционной системы вы также можете использовать менеджеры пакетов rpm, dpkg или dnf для установки Агента администрирования.

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

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 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.

Установка Агента администрирования для Linux в интерактивном режиме

В этой статье описывается, как установить Агент администрирования на устройства с операционной системой Linux в интерактивном режиме, указав параметры установки шаг за шагом. Вы также можете использовать файл ответов – текстовый файл, который содержит пользовательский набор параметров установки: переменные и их соответствующие значения. Использование файла ответов позволяет запустить установку в тихом режиме, то есть без участия пользователя.

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

Чтобы установить Агент администрирования в интерактивном режиме:

1. Запустите инсталляционный пакет Агент администрирования. В зависимости от вашего дистрибутива Linux выполните одну из следующих команд:

   - Чтобы установить Агент администрирования из RPM-пакета на устройство с 32-битной операционной системой:

     `# yum -i klnagent-<номер сборки>.i386.rpm`

   - Чтобы установить Агент администрирования из RPM-пакета на устройство с 64-битной операционной системой:

     `# yum -i klnagent64-<номер сборки>.x86_64.rpm`

   - Чтобы установить Агент администрирования из RPM-пакета на устройство с 64-битной операционной системой для Arm-архитектуры:

     `# yum -i klnagent64-<номер сборки>.aarch64.rpm`

   - Чтобы установить Агент администрирования из DEB-пакета на устройство с 32-битной операционной системой:

     `# apt install ./klnagent_<номер сборки>_i386.deb`

   - Чтобы установить Агент администрирования из DEB-пакета на устройство с 64-битной операционной системой:

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

   - Чтобы установить Агент администрирования из DEB-пакета на устройство с 64-битной операционной системой для Arm-архитектуры:

     `# apt install ./klnagent64_<номер сборки>_arm64.deb`

2. Запустите настройку Агента администрирования:

   `# /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl`

3. Прочитайте Лицензионное соглашение. Текст отображается в окне командной строки. Нажмите пробел, чтобы просмотреть следующий фрагмент текста. При отображении запроса введите одно из следующих значений:

   - Введите `y`, если вы понимаете и принимаете условия Лицензионного соглашения.

   - Введите `n`, если вы не принимаете условия Лицензионного соглашения. Чтобы использовать Агент администрирования, вам нужно принять условия Лицензионного соглашения.

   - Введите `r`, чтобы снова отобразить Лицензионное соглашение.

4. Введите DNS-имя Сервера администрирования или IP-адрес.

5. Введите номер порта Сервера администрирования. По умолчанию номер порта – 14000.

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

7. Введите `y`, если вы хотите использовать SSL-шифрование для трафика между Агентом администрирования и Сервером администрирования. Иначе введите `n`.

8. Выберите один из следующих способов настройки Агента администрирования:

   - `[1]` – не настраивать шлюз соединения.

     Ваше устройство не будет выступать в роли шлюза соединения и не будет подключаться к Серверу администрирования через шлюз соединения.

   - `[2]` – не использовать шлюз соединения.

     Ваше устройство не будет подключаться к Серверу администрирования через шлюз соединения.

   - `[3]` – подключитесь к Серверу с помощью шлюза соединения.

     Ваше устройство будет подключаться к Серверу администрирования через шлюз соединения.

   - `[4]` – использовать в качестве шлюза соединения.

     Ваше устройство будет выступать в роли шлюза соединения.

Агент администрирования установлен на устройстве с операционной системой Linux.

Локальная установка плагина управления приложением

Чтобы установить плагин управления приложением,

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

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

Установка приложений в тихом режиме

Чтобы установить приложение в тихом режиме:

1. Откройте главное окно приложения Kaspersky Security Center.

2. В папке дерева консоли **Удаленная установка** во вложенной папке **Инсталляционные пакеты** выберите инсталляционный пакет нужного приложения или сформируйте для этого приложения новый инсталляционный пакет.

   Инсталляционный пакет будет сохранен на Сервере администрирования в папке общего доступа в служебной папке Packages. При этом каждому инсталляционному пакету соответствует отдельная вложенная папка.

3. Откройте папку нужного инсталляционного пакета одним из следующих способов:

   - Скопируйте папку, соответствующую нужному инсталляционному пакету, с Сервера администрирования на клиентское устройство. Затем откройте скопированную папку на клиентском устройстве.

   - С клиентского устройства откройте на Сервере администрирования папку общего доступа, соответствующую нужному инсталляционному пакету.

   Если папка общего доступа расположена на устройстве с установленной операционной системой Microsoft Windows Vista, необходимо установить значение **Выключено** для параметра **Управление учетными записями пользователей: все администраторы работают в режиме одобрения администратором** (**Пуск** → **Панель управления** → **Администрирование** → **Локальная политика безопасности** → **Параметры безопасности**).

4. В зависимости от выбранного приложения выполните следующие действия:

   - Для Антивируса Касперского для Windows Workstations, Антивируса Касперского для Windows Servers и Kaspersky Security Center перейдите во вложенную папку exec и запустите исполняемый файл (файл с расширением exe) с ключом /s.

   - Для остальных приложений "Лаборатории Касперского" запустите из открытой папки исполняемый файл (файл с расширением exe) с ключом /s.

   Запуск исполняемого файла с ключами `EULA=1` и `PRIVACYPOLICY=1` означает, что вы полностью прочитали, поняли и принимаете положения Лицензионного соглашения и Политики конфиденциальности соответственно. Вам также известно, что ваши данные будут обрабатываться и передаваться (в том числе в третьи страны), как описано в Политике конфиденциальности. Текст Лицензионного соглашения и текст Политики конфиденциальности входят в комплект поставки Kaspersky Security Center. Согласие с положениями Лицензионного соглашения и Политики конфиденциальности является необходимым условием для установки приложения или обновления предыдущей версии приложения.

Установка приложений с помощью автономных пакетов

Kaspersky Security Center позволяет формировать автономные инсталляционные пакеты приложений. Автономный инсталляционный пакет представляет собой исполняемый файл, который можно разместить на Веб-сервере, отправить по почте или передать на клиентское устройство другим способом. Полученный файл можно запустить локально на клиентском устройстве для выполнения установки приложения без участия Kaspersky Security Center.

Автономный инсталляционный пакет Агент администрирования для Linux имеет дополнительную зависимость от утилиты nmap. Если утилита nmap отсутствует или имеет версию ниже 6.0, функциональность Broadcast DHCP Discover не поддерживается.

Чтобы установить приложение с помощью автономного инсталляционного пакета:

1. Подключитесь к нужному Серверу администрирования.

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

3. В рабочей области выберите инсталляционный пакет нужного приложения.

4. Запустите процесс создания автономного инсталляционного пакета одним из следующих способов:

   - В контекстном меню инсталляционного пакета выберите пункт **Создать автономный инсталляционный пакет**.
   - Перейдите по ссылке **Создать автономный инсталляционный пакет** в рабочей области инсталляционного пакета.

   Запустится мастер создания автономного инсталляционного пакета. Следуйте далее указаниям мастера.

   На завершающем шаге мастера выберите способ передачи автономного инсталляционного пакета на клиентское устройство.

5. Передайте автономный инсталляционный пакет приложения на клиентское устройство.

6. Запустите автономный инсталляционный пакет на клиентском устройстве.

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

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

Параметры инсталляционного пакета Агента администрирования

Чтобы настроить параметры инсталляционного пакета Агента администрирования:

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

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

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

   Откроется окно свойств инсталляционного пакета Агента администрирования.

Общие

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

- название инсталляционного пакета;
- имя и версию приложения, для которого сформирован инсталляционный пакет;
- размер инсталляционного пакета;
- дата создания инсталляционного пакета;
- путь к папке размещения инсталляционного пакета.

Settings

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**

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

  По умолчанию пароль не установлен.

- **Защитить службу Агента администрирования от неавторизованного удаления, остановки или изменения параметров работы**

  Если этот параметр включен, после того, как Агент администрирования был установлен на управляемом устройстве, компонент не может быть удален или изменен без требуемых прав. Работа Агента администрирования не может быть остановлена. Этот параметр не влияет на контроллеры домена.

  Включите этот параметр, чтобы защитить Агент администрирования на рабочих станциях, управляемых с правами локального администратора.

  По умолчанию параметр выключен.

- **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**

  Если этот параметр включен, все загруженные обновления и патчи для Сервера администрирования, Агента администрирования, Консоли администрирования и Сервера iOS MDM будут установлены автоматически.

  Если этот параметр выключен, то загруженные обновления и патчи будут установлены только после того, как вы измените их статус на *Одобрено*. Обновления и патчи со статусом *Не определено* не будут установлены.

  По умолчанию параметр включен.

Подключение

В этом разделе можно настроить параметры подключения Агента администрирования к Серверу администрирования. Для установления соединения можно использовать SSL-протокол или UDP-протокол. Для настройки соединения укажите следующие параметры:

- **Сервер администрирования**

  Адрес устройства, на котором установлен Сервер администрирования.

- **Порт**

  Номер порта, по которому будет выполняться подключение.

- **SSL-порт**

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

- **Использовать сертификат Сервера**

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

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

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

  По умолчанию флажок установлен.

- **Использовать SSL**

  Если этот параметр включен, подключение к Серверу администрирования будет выполняться через защищенный порт с использованием TLS-протокола.

  По умолчанию параметр выключен. Чтобы ваше соединение оставалось безопасным, рекомендуется не выключать этот параметр.

- **Использовать UDP-порт**

  Если этот параметр включен, подключение Агента администрирования к Серверу администрирования будет выполняться через UDP-порт. Это позволяет управлять клиентскими устройствами и получать информацию о них.

  UDP-порт должен быть открыт на управляемых устройствах, на которых установлен Агент администрирования. Поэтому рекомендуется не выключать этот параметр.

  По умолчанию параметр включен.

- **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.

- **Использовать прокси-сервер**

  Если этот параметр включен, укажите параметры прокси-сервера:

  - **Адрес прокси-сервера**
  - **Порт прокси-сервера**

  Если ваш прокси-сервер требует аутентификации, включите параметр **Аутентификация на прокси-сервере** и укажите **Имя пользователя** и **Пароль** учетной записи, под которой установлено соединение с прокси-сервером. Рекомендуется указывать данные учетной записи с минимальными правами, необходимыми только для аутентификации на прокси-сервере.

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

Дополнительно

В разделе **Дополнительно** вы можете настроить как использовать шлюз соединения. Для этого можно выполнить следующие действия:

- Используйте Агент администрирования в качестве шлюза соединения в демилитаризованной зоне (DMZ) для подключения к Серверу администрирования, связи с ним и сохранения данных в безопасности на Агенте администрирования, во время передачи данных.

- **Подключайтесь к Серверу администрирования с помощью шлюза соединения**, чтобы уменьшить количество подключений к Серверу администрирования. В этом случае введите адрес устройства, которое будет выступать в качестве шлюза соединения в поле **Адрес шлюза соединения**.

  Поддерживается только прямое подключение к шлюзу соединения. Параметр использования интернет-прокси-сервера, указанный в инсталляционном пакете, не применяется.

- Настройте подключение для Virtual Desktop Infrastructure (VDI), если в вашей сети есть виртуальные машины. Для этого выполните следующее:

  - **Включить динамический режим для VDI**

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

    По умолчанию параметр выключен.

  - **Оптимизировать параметры для VDI**

    Если параметр включен, в параметрах Агента администрирования выключены следующие функции:

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

    По умолчанию параметр выключен.

- **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 параметров **Открывать порты Агента администрирования в брандмауэре Microsoft Windows** и **Использовать только автоматическое определение прокси-сервера**)	✓ (кроме параметров **Открывать порты Агента администрирования в брандмауэре Microsoft Windows** и **Использовать только автоматическое определение прокси-сервера**)
Дополнительно	✓	✓	✓
Дополнительные компоненты	✓	✓	✓
Теги	✓	✓ (кроме правил автоматического назначения тегов)	✓ (кроме правил автоматического назначения тегов)
История ревизий	✓	✓	✓

Просмотр Политики конфиденциальности

Политика конфиденциальности доступна в интернете на странице https://www.kaspersky.ru/products-and-services-privacy-policy; также она доступна в офлайн-режиме. Вы можете ознакомиться с Политикой конфиденциальности, например, перед установкой Агента администрирования.

Чтобы прочитать Политику конфиденциальности в офлайн-режиме:

1. Запустите установщик Kaspersky Security Center.
2. В окне установщика перейдите по ссылке **Извлечь инсталляционные пакеты**.
3. В открывшемся списке выберите Агент администрирования Kaspersky Security Center и нажмите на кнопку **Далее**.

Файл privacy_policy.txt появится на вашем устройстве в указанной вами папке в подпапке NetAgent.

Развертывание систем управления мобильными устройствами

В этом разделе описано развертывание систем управления мобильных устройств по протоколам iOS MDM и Kaspersky Endpoint Security.

Развертывание системы управления по протоколу iOS MDM

Kaspersky Security Center позволяет управлять мобильными устройствами на платформе iOS. Мобильными устройствами iOS MDM называются мобильные устройства iOS, подключенные к Серверу iOS MDM и находящиеся под управлением Сервера администрирования.

Подключение мобильных устройств к Серверу iOS MDM выполняется в следующей последовательности:

1. Администратор устанавливает Сервер iOS MDM.
2. Администратор получает сертификат сервиса Apple Push Notification Service (APNs) (Получение APNs-сертификата, https://support.kaspersky.com/help/KSMM/4.1/en-US/64900.htm).

   APNs-сертификат позволяет Серверу администрирования подключаться к серверу APNs для отправки push-уведомлений на устройства iOS MDM.
3. Администратор устанавливает на Сервере iOS MDM APNs-сертификат.
4. Администратор формирует iOS MDM-профиль для пользователя мобильного устройства iOS.

   Профиль iOS MDM содержит набор параметров для подключения мобильных устройств iOS к Серверу администрирования.

После установки профиля и синхронизации мобильного устройства iOS MDM с Сервером администрирования устройство отображается в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Установка Сервера iOS MDM

Чтобы установить Сервер iOS MDM на локальное устройство:

1. Запустите исполняемый файл setup.exe.

Откроется окно с выбором приложений "Лаборатории Касперского" для установки.

В окне с выбором приложений по ссылке **Установить Сервер iOS MDM** запустите мастер установки Сервера iOS MDM.

2. Выберите папку назначения.

   Папка назначения по умолчанию <Диск>:\Program Files\Kaspersky Lab\Mobile Device Management for iOS. Если такой папки нет, она будет создана автоматически в процессе установки. Вы можете изменить папку назначения с помощью кнопки **Обзор**.

3. В окне мастера **Параметры подключения к Серверу iOS MDM** в поле **Внешний порт подключения к службе iOS MDM** укажите внешний порт для подключения мобильных устройств к службе iOS MDM.

   Внешний порт 5223 используется мобильными устройствами для связи с APNs-сервером. Убедитесь, что в сетевом экране открыт порт 5223 для подключения к диапазону адресов 17.0.0.0/8.

   Для подключения устройства к Серверу iOS MDM по умолчанию используется порт 443. Если порт 443 уже используется другим сервисом или приложением, то его можно изменить, например, на порт 9443.

   Сервер iOS MDM использует внешний порт 2197 для отправки уведомлений на APNs-сервер.

   APNs-серверы работают в режиме сбалансированной нагрузки. Мобильные устройства не всегда подключаются к одним и тем же IP-адресам для получения уведомлений. Диапазон адресов 17.0.0.0/8 назначен компании Apple, поэтому рекомендуется указать весь этот диапазон как разрешенный в параметрах сетевого экрана.

4. Если вы хотите вручную настроить порты для взаимодействия между компонентами приложения, выберите параметр **Настроить локальные порты вручную**, а затем укажите значения следующих параметров:

   - **Порт подключения к Агенту администрирования**. Укажите в поле порт подключения службы iOS MDM к Агенту администрирования. По умолчанию установлен порт 9799.
   - **Локальный порт подключения к службе iOS MDM**. Укажите в поле локальный порт подключения Агента администрирования к службе iOS MDM. По умолчанию установлен порт 9899.

   Рекомендуется использовать значения по умолчанию.

5. В окне мастера **Внешний адрес Сервера мобильных устройств** в поле **Веб-адрес удаленного соединения с Сервером мобильных устройств** укажите адрес клиентского устройства, на котором будет установлен Сервер iOS MDM.

   Этот адрес будет использоваться для подключения управляемых мобильных устройств к службе iOS MDM. Клиентское устройство должно быть доступно для подключения к нему iOS MDM-устройств.

   Вы можете указать адрес клиентского устройства в одном из следующих форматов:

   - FQDN-имя устройства (например, mdm.example.com);
   - NetBIOS-имя устройства.

   Не следует включать в строку с адресом URL-схему и номер порта: эти значения будут добавлены автоматически.

В результате работы мастера Сервер iOS MDM будет установлен на локальное устройство. Сервер iOS MDM отображается в папке **Управление мобильными устройствами** дерева консоли.

Установка Сервера iOS MDM в тихом режиме

Kaspersky Security Center позволяет устанавливать Сервер iOS MDM на локальное устройство в тихом режиме, то есть без интерактивного ввода параметров установки.

Чтобы установить Сервер iOS MDM на локальное устройство в тихом режиме:

1. Прочитайте Лицензионное соглашение. Используйте команду ниже, только если вы поняли и принимаете условия Лицензионного соглашения.

2. Выполните следующую команду:

   ```
   .\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 <installation_settings>"
   ```

   где `setup_parameters` – перечень параметров и их значений, отделенных друг от друга пробелом (`PROP1=PROP1VAL PROP2=PROP2VAL`). Файл setup.exe расположен в папке Server внутри дистрибутива Kaspersky Security Center.

Имена и возможные значения параметров, которые можно использовать при установке Сервера iOS MDM в тихом режиме, приведены в таблице ниже. Параметры можно указывать в любом порядке.

Параметры установки Сервера iOS MDM в тихом режиме

Имя параметра	Описание параметра	Доступные значения
EULA	Согласие с условиями Лицензионного соглашения. Этот параметр является обязательным.	• 1 – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Лицензионного соглашения. • Другое значение или не задано – не согласны с условиями Лицензионного соглашения (установка не выполняется).
DONT_USE_ANSWER_FILE	Использовать xml-файл с параметрами установки Сервера iOS MDM или нет. xml-файл идет в комплекте с инсталляционным пакетом или находится на Сервере администрирования. Дополнительно путь к файлу указывать не нужно. Этот параметр является обязательным.	• 1 – не использовать XML-файл с параметрами. • Другое значение или не задано – использовать XML-файл с параметрами.
INSTALLDIR	Папка установки Сервера iOS MDM. Этот параметр является необязательным.	Строковое значение, например, `INSTALLDIR=\"C:\install\"`
CONNECTORPORT	Локальный порт подключения службы iOS MDM к Агенту администрирования. По умолчанию установлен порт 9799. Этот параметр является необязательным.	Числовое значение.
LOCALSERVERPORT	Локальный порт подключения Агента администрирования к службе iOS MDM. По умолчанию установлен порт 9899. Этот параметр является необязательным.	Числовое значение.
EXTERNALSERVERPORT	Порт для подключения устройства к Серверу iOS MDM. По умолчанию установлен порт 443. Этот параметр является необязательным.	Числовое значение.
EXTERNAL_SERVER_URL	Внешний адрес клиентского устройства, на котором будет установлен Сервер iOS MDM. Этот адрес будет использоваться для подключения управляемых мобильных устройств к службе iOS MDM. Клиентское устройство должно быть доступно для подключения к нему iOS MDM. Адрес не должен включать URL-схему и номер порта, так как эти значения будут добавлены автоматически. Этот параметр является необязательным.	• FQDN-имя устройства (например, mdm.example.com); • NetBIOS-имя устройства; • IP-адрес устройства.

Имя параметра	Описание параметра	Доступные значения
WORKFOLDER	Рабочая папка Сервера iOS MDM. Если рабочая папка не указана, данные будут записаны в папку по умолчанию. Этот параметр является необязательным.	Строковое значение, например, `WORKFOLDER=\"C:\work\"`
MTNCY	Использование Сервера iOS MDM несколькими виртуальными Серверами. Этот параметр является необязательным.	• 1 – Сервер iOS MDM будет использоваться несколькими виртуальными Серверами администрирования. • Другое значение или не задано – Сервер iOS MDM не будет использоваться несколькими виртуальными Серверами администрирования.

Пример:
```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443 EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

Параметры установки Сервера iOS MDM подробно описаны в разделе "Установка Сервера iOS MDM".

Схемы развертывания Сервера iOS MDM

Количество установленных копий Сервера iOS MDM может быть выбрано как исходя из наличия доступного аппаратного обеспечения, так и в зависимости от общего количества обслуживаемых мобильных устройств.

Следует учесть, что на одну установку Kaspersky Device Management для iOS рекомендуется не более 50 000 мобильных устройств. С целью уменьшения нагрузки все множество устройств можно распределить между несколькими серверами с установленным Сервером iOS MDM.

Аутентификация iOS MDM-устройств осуществляется при помощи пользовательских сертификатов (профиль, устанавливаемый на устройство, содержит сертификат того пользователя, которому оно принадлежит). Поэтому возможны две схемы развертывания Сервера iOS MDM:

- упрощенная схема;
- схема развертывания с использованием принудительного делегирования Kerberos Constrained Delegation (KCD).

Упрощенная схема развертывания

При развертывании Сервера iOS MDM по упрощенной схеме мобильные устройства напрямую подключаются к веб-службе iOS MDM. При этом для аутентификации устройств могут быть использованы только пользовательские сертификаты, выпущенные Сервером администрирования. Интеграция с инфраструктурой открытых ключей (Public Key Infrastructure, PKI) для пользовательских сертификатов невозможна.

Схема развертывания с использованием принудительного делегирования Kerberos Constrained Delegation (KCD)

Чтобы использовать схему развертывания с ограниченным делегированием Kerberos (KCD), должны быть выполнены следующие требования:

- Сервер администрирования и Сервер iOS MDM располагаются во внутренней сети организации.
- Используется обратный прокси-сервер с поддержкой KCD.

Эта схема развертывания предполагает:

- интеграцию с обратным прокси-сервером, поддерживающим KCD;
- использование для аутентификации мобильных устройств принудительного делегирования Kerberos Constrained Delegation;
- интеграцию с инфраструктурой открытых ключей (PKI) для использования пользовательских сертификатов.

При использовании этой схемы развертывания следует учесть следующее:

- В Консоли администрирования в параметрах веб-службы iOS MDM необходимо установить флажок **Обеспечить совместимость с Kerberos constrained delegation**.
- В качестве сертификата веб-службы iOS MDM следует указать особый (кастомизированный) сертификат, заданный на TMG при публикации на обратном прокси-сервере.
- Пользовательские сертификаты для iOS-устройств должны выписываться доменным Центром сертификации (Certification authority, далее CA). Если в домене несколько корневых CA, то пользовательские сертификаты должны быть выписаны CA, указанным при публикации веб-службы iOS MDM на обратном прокси-сервере.

  Обеспечить соответствие пользовательского сертификата указанному требованию возможно несколькими способами:

  - Указать пользовательский сертификат в мастере создания iOS MDM-профиля и в мастере установки сертификатов.
  - Интегрировать Сервер администрирования с доменным PKI и настроить соответствующий параметр в правилах выписки сертификатов:

    1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Сертификаты**.
    2. В рабочей области папки **Сертификаты** по кнопке **Настроить правила выпуска сертификатов** откройте окно **Правила выпуска сертификатов**.
    3. В разделе **Интеграция с PKI** настройте интеграцию с инфраструктурой открытых ключей.
    4. В разделе **Выпуск мобильных сертификатов** укажите источник сертификатов.

Рассмотрим пример настройки ограниченного делегирования KCD со следующими допущениями:

- веб-служба iOS MDM запущена на 443 порте;
- имя устройства с обратным прокси-сервером – firewall.mydom.local;
- имя устройства с веб-службой iOS MDM – iosmdm.mydom.local;
- имя внешней публикации веб-службы iOS MDM – iosmdm.mydom.global.

Service Principal Name для http/iosmdm.mydom.local

В домене требуется прописать Service Principal Name (SPN) для устройства с веб-службой iOS MDM (iosmdm.mydom.local):

```
setspn -a http/iosmdm.mydom.local iosmdm
```

Настройка доменных свойств устройств с обратным прокси-сервером (firewall.mydom.local)

Для делегирования трафика можно доверить устройство с обратным прокси-сервером (firewall.mydom.local) службе, определенной по SPN (http/iosmdm.mydom.local).

Чтобы доверить устройство с обратным прокси-сервером службе, определенной по SPN (http/iosmdm.mydom.local), администратору нужно выполнить следующие действия:

1. В оснастке Microsoft Management Console "Active Directory Users and Computers" выбрать устройство с установленным обратным прокси-сервером (firewall.mydom.local).
2. В свойствах устройства на вкладке **Delegation** для переключателя **Trust this computer for delegation to specified service only** выбрать вариант **Use any authentication protocol**.
3. В список **Services to which this account can present delegated credentials** добавить SPN http/iosmdm.mydom.local.

Особый (кастомизированный) сертификат для публикуемой веб-службы (iosmdm.mydom.global)

Требуется выписать особый (кастомизированный) сертификат для веб-службы iOS MDM на FQDN iosmdm.mydom.global и указать его взамен сертификата по умолчанию в параметрах веб-службы iOS MDM в Консоли администрирования.

Следует учесть, что в контейнере с сертификатом (файл с расширением p12 или pfx) также должна присутствовать цепочка корневых сертификатов (публичные части).

Публикации веб-службы iOS MDM на обратном прокси-сервере

На обратном прокси-сервере для трафика, идущего со стороны мобильного устройства на 443 порт iosmdm.mydom.global, необходимо настроить KCD на SPN (http/iosmdm.mydom.local) с использованием сертификата, выписанного для FQDN (iosmdm.mydom.global). При этом следует учесть, что как на публикации, так и на публикуемой веб-службе должен быть один и тот же серверный сертификат.

Получение APNs-сертификата

Если у вас уже есть APNs-сертификат, обновите его, вместо создания нового. При замене существующего APNs-сертификата на вновь созданный Сервер администрирования теряет управление над подключенными в данный момент мобильными устройствами iOS.

После создания запроса Certificate Signing Request (далее CSR-запрос) на первом шаге мастера получения APNs-сертификата приватная часть будущего сертификата (private key) сохраняется в оперативной памяти устройства. Поэтому все шаги мастера должны быть завершены в рамках одного сеанса работы с приложением.

Чтобы получить APNs-сертификат:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
2. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
3. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера iOS MDM.
4. В окне свойств Сервера iOS MDM выберите раздел **Сертификаты**.
5. В разделе **Сертификаты** в блоке параметров **Сертификат Apple Push Notification** нажмите на кнопку **Запросить новый**.

   Запустится мастер получения APNs-сертификата, откроется окно **Запросить новый**.
6. Создайте запрос Certificate Signing Request (далее CSR-запрос). Для этого выполните следующие действия:

   a. Нажмите на кнопку **Создать CSR**.

   b. В открывшемся окне **Создание CSR** укажите название запроса, название компании и департамента, город, область и страну.

   c. Нажмите на кнопку **Сохранить** и укажите имя файла, в котором будет сохранен CSR-запрос.

   Приватная часть (private key) будущего сертификата будет сохранена в памяти устройства.
7. Отправьте созданный файл с CSR-запросом на подпись в "Лабораторию Касперского" через ваш CompanyAccount.

   Подписание CSR-запроса доступно только после загрузки на портал CompanyAccount ключа, разрешающего использование Управления мобильными устройствами.

   После обработки вашего электронного запроса вы получите файл CSR-запроса, подписанный "Лабораторией Касперского".
8. Отправьте подписанный файл CSR-запроса на веб-сайт Apple Inc., используя произвольный Apple ID.

Не рекомендуется использовать персональный Apple ID. Создайте отдельный Apple ID, чтобы использовать его как корпоративный. Созданный Apple ID привяжите к почтовому ящику организации, а не отдельного сотрудника.

После обработки CSR-запроса в Apple Inc. вы получите публичную часть APNs-сертификата. Сохраните полученный файл на диск.

9. Экспортируйте APNs-сертификат вместе с приватным ключом, созданным при формировании CSR-запроса, в файл формата PFX. Для этого выполните следующие действия:

   a. В окне **Запрос нового APNs-сертификата** нажмите на кнопку **Завершить CSR**.

   b. В открывшемся окне **Открыть** выберите файл с публичной частью сертификата, полученный после обработки CSR-запроса в Apple Inc., и нажмите на кнопку **Открыть**.

      Запустится экспорт сертификата.

   c. В открывшемся окне введите пароль для приватного ключа, нажмите на кнопку **OK**.

      Заданный пароль будет использоваться для установки APNs-сертификата на Сервер iOS MDM.

   d. В открывшемся окне **Сохранение APNs-сертификата** укажите имя файла для сохранения APNs-сертификата, выберите папку, в которую он будет сохранен, и нажмите на кнопку **Сохранить**.

Приватная и публичная части сертификата будут объединены, APNs-сертификат будет сохранен в файл формата PFX. После этого вы можете установить на Сервере iOS MDM APNs-сертификат.

Обновление APNs-сертификата

Чтобы обновить APNs-сертификат:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.

2. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.

3. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера iOS MDM.

4. В окне свойств Сервера iOS MDM выберите раздел **Сертификаты**.

5. В разделе **Сертификаты** в блоке параметров **Сертификат Apple Push Notification** нажмите на кнопку **Обновить**.

   Запустится мастер обновления APNs-сертификата, откроется окно **Обновление APNs-сертификата**.

6. Создайте запрос Certificate Signing Request (далее CSR-запрос). Для этого выполните следующие действия:

   a. Нажмите на кнопку **Создать CSR**.

   b. В открывшемся окне **Создание CSR** укажите название запроса, название компании и департамента, город, область и страну.

   c. Нажмите на кнопку **Сохранить** и укажите имя файла, в котором будет сохранен CSR-запрос.

Приватная часть (private key) будущего сертификата будет сохранена в памяти устройства.

7. Отправьте созданный файл с CSR-запросом на подпись в "Лабораторию Касперского" через ваш CompanyAccount.

   Подписание CSR-запроса доступно только после загрузки на портал CompanyAccount ключа, разрешающего использование Управления мобильными устройствами.

   После обработки вашего электронного запроса вы получите файл CSR-запроса, подписанный "Лабораторией Касперского".

8. Отправьте подписанный файл CSR-запроса на веб-сайт Apple Inc., используя произвольный Apple ID.

   Не рекомендуется использовать персональный Apple ID. Создайте отдельный Apple ID, чтобы использовать его как корпоративный. Созданный Apple ID привяжите к почтовому ящику организации, а не отдельного сотрудника.

   После обработки CSR-запроса в Apple Inc. вы получите публичную часть APNs-сертификата. Сохраните полученный файл на диск.

9. Запросите публичную часть сертификата. Для этого выполните следующие действия:

   a. Перейдите на портал Apple Push Certificates. Для авторизации на портале потребуется Apple Id, полученный при первичном запросе сертификата.

   b. В списке сертификатов выберите сертификат, APSP-имя которого (имя в формате "APSP: <номер>") совпадает с APSP-именем сертификата, используемого Сервером iOS MDM, и нажмите на кнопку **Обновить**.

      APNs-сертификат будет обновлен.

   c. Сохраните созданный порталом сертификат.

10. Экспортируйте APNs-сертификат вместе с приватным ключом, созданным при формировании CSR-запроса, в файл формата PFX. Для этого выполните следующие действия:

    a. В окне **Обновление APNs-сертификата** нажмите на кнопку **Завершить CSR**.

    b. В открывшемся окне **Открыть** выберите файл с публичной частью сертификата, полученный после обработки CSR-запроса в Apple Inc., и нажмите на кнопку **Открыть**.

       Запустится экспорт сертификата.

    c. В открывшемся окне введите пароль для приватного ключа, нажмите на кнопку **OK**.

       Заданный пароль будет использоваться для установки APNs-сертификата на Сервер iOS MDM.

    d. В открывшемся окне **Обновление APNs-сертификата** укажите имя файла для сохранения APNs-сертификата, выберите папку, в которую он будет сохранен, и нажмите на кнопку **Сохранить**.

Приватная и публичная части сертификата будут объединены, APNs-сертификат будет сохранен в файл формата PFX.

Настройка резервного сертификата Сервера iOS MDM

Функциональность Сервера iOS MDM позволяет выписать резервный сертификат. Этот сертификат предназначен для использования в iOS MDM-профилях, чтобы обеспечить переключение управляемых iOS-устройств после истечения срока действия сертификата Сервера iOS MDM.

Если ваш Сервер iOS MDM использует сертификат выданный "Лабораторией Касперского" по умолчанию, вы можете выпустить резервный сертификат (или указать свой собственный сертификат в качестве резервного) до истечения срока действия сертификата Сервера iOS MDM. По умолчанию резервный сертификат автоматически выпускается за 60 дней до истечения срока действия сертификата Сервера iOS MDM. Резервный сертификат Сервера iOS MDM становится основным сразу после истечения срока действия сертификата Сервера iOS MDM. Открытый ключ распространяется на все управляемые устройства через конфигурационные профили, поэтому вам не нужно передавать его вручную.

Чтобы выпустить резервный сертификат Сервера iOS MDM или указать пользовательский резервный сертификат:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.

2. В списке Серверов мобильных устройств выберите соответствующий Сервер iOS MDM и на правой панели нажмите на кнопку **Настроить параметры Сервера iOS MDM**.

3. В открывшемся окне свойств Сервера iOS MDM выберите раздел **Сертификаты**.

4. В блоке параметров **Резервный сертификат** выполните одно из следующих действий:

   - Если вы планируете и дальше использовать самоподписанный сертификат (то есть выписанный "Лабораторией Касперского"):

     a. Нажмите на кнопку **Выпуск**.

     b. В открывшемся окне **Дата активации** выберите один из двух вариантов даты, когда необходимо применить резервный сертификат:

        - Если вы хотите применить резервный сертификат в момент истечения срока действия текущего сертификата, выберите параметр **Дата истечения срока действия текущего сертификата**.

        - Если вы хотите применить резервный сертификат до истечения срока действия текущего сертификата, выберите параметр **После указанного периода (сут)**. В поле ввода рядом с этим параметром укажите продолжительность периода, по истечении которого резервный сертификат должен заменить текущий сертификат.

     > Срок действия указанного вами резервного сертификата не может превышать срок действия текущего сертификата Сервера iOS MDM.

     c. Нажмите на кнопку **OK**.

   Резервный сертификат Сервера iOS MDM выпущен.

- Если вы планируете использовать пользовательский сертификат, выпущенный доверенным центром сертификации:

  a. Нажмите на кнопку **Добавить**.

  b. В открывшемся окне проводника укажите файл сертификата в формате PEM, PFX или P12, который хранится на вашем устройстве, и нажмите на кнопку **Открыть**.

  Пользовательский сертификат указан как резервный сертификат Сервера iOS MDM.

Резервный сертификат Сервера iOS MDM указан. Подробная информация о резервном сертификате отображается в блоке параметров **Резервный сертификат** (название сертификата, название того, кто выписал сертификат, срок действия и дата применения резервного сертификата, если есть).

Установка APNs-сертификата на Сервер iOS MDM

После получения APNs-сертификата необходимо установить APNs-сертификат на Сервер iOS MDM.

Чтобы установить APNs-сертификат на Сервер iOS MDM:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
2. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
3. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера iOS MDM.
4. В окне свойств Сервера iOS MDM выберите раздел **Сертификаты**.
5. В разделе **Сертификаты** в блоке параметров **Сертификат Apple Push Notification** нажмите на кнопку **Установить**.
6. Выберите файл формата PFX, содержащий APNs-сертификат.
7. Введите пароль приватного ключа, указанный при экспорте APNs-сертификата.

В результате APNs-сертификат будет установлен на Сервер iOS MDM. Информация о сертификате будет отображаться в окне свойств Сервера iOS MDM в разделе **Сертификаты**.

Настройка доступа к сервису Apple Push Notification

Для корректной работы веб-службы iOS MDM, а также для обеспечения своевременного реагирования мобильных устройств на команды администратора, в параметрах Сервера iOS MDM следует указать сертификат Apple Push Notification Service (далее APNs-сертификат).

Взаимодействуя с сервисом Apple Push Notification (далее APNs), веб-служба iOS MDM подключается к внешнему адресу api.push.apple.com по порту 2197 (исходящий). Поэтому веб-службе iOS MDM необходимо предоставить доступ к порту TCP 2197 для диапазона адресов 17.0.0.0/8. Со стороны iOS-устройства – доступ к порту TCP 5223 для диапазона адресов 17.0.0.0/8.

Если доступ к APNs со стороны веб-службы iOS MDM предполагается осуществлять через прокси-сервер, то на устройстве с установленным веб-службой iOS MDM необходимо выполнить следующие действия:

1. Прописать в Реестр следующие строки:

   - Для 32-разрядной операционной системы:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<Proxy Host Name>"
"ApnProxyPort"="<Proxy Port>"
"ApnProxyLogin"="<Proxy Login>"
"ApnProxyPwd"="<Proxy Password>"
```

   - Для 64-разрядной операционной системы:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<Proxy Host Name>"
"ApnProxyPort"="<Proxy Port>"
"ApnProxyLogin"="<Proxy Login>"
"ApnProxyPwd"="<Proxy Password>"
```

2. Перезапустить веб-службу iOS MDM.

Выписка и установка общего сертификата на мобильное устройство

Чтобы выписать общий сертификат пользователю:

1. В дереве консоли в папке **Учетные записи пользователей** выберите учетную запись пользователя.

2. В контекстном меню учетной записи пользователя выберите пункт **Установить сертификат**.

   Будет запущен мастер установки сертификата. Следуйте далее указаниям мастера.

В результате работы мастера сертификат будет создан и добавлен в список пользовательских сертификатов.

Выписанный сертификат пользователь загружает вместе с установочным пакетом, в котором содержится iOS MDM-профиль.

После подключения мобильного устройства к Серверу iOS MDM на устройстве пользователя будут применены параметры iOS MDM-профиля. Администратор сможет управлять подключенным устройством.

Мобильное устройство пользователя, подключенное к Серверу iOS MDM, отображается в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Добавление KES-устройства в список управляемых устройств

Чтобы добавить KES-устройство пользователя в список управляемых устройств с помощью ссылки на Google Play™:

1. В дереве консоли выберите папку **Учетные записи пользователей**.

   По умолчанию папка **Учетные записи пользователей** вложена в папку **Дополнительно**.

2. Выберите учетную запись пользователя, мобильное устройство которого вы хотите добавить в список управляемых устройств.

3. В контекстном меню учетной записи пользователя выберите пункт **Добавить мобильное устройство**.

   Запустится мастер подключения мобильного устройства. В окне мастера **Источник сертификата** требуется указать способ создания общего сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Вы можете задать общий сертификат одним из двух способов:

   - автоматически создать общий сертификат средствами Сервера администрирования и доставить сертификат на устройство;
   - указать файл общего сертификата.

4. В окне мастера **Тип устройства** выберите вариант **Ссылка на Google Play**.

5. В окне мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата (с помощью SMS-сообщения, по электронной почте или информация будет отображена после окончания работы мастера).

6. В окне мастера Информация о сертификате нажмите на кнопку **Готово** для завершения работы мастера.

В результате работы мастера на устройство пользователя будет отправлена ссылка и QR-код для загрузки Kaspersky Endpoint Security для Android с Google Play. Пользователь переходит в магазин приложений Google Play по ссылке или отсканировав QR-код. После этого операционная система устройства запрашивает у пользователя согласие на установку Kaspersky Endpoint Security для Android. После загрузки и установки Kaspersky Endpoint Security для Android мобильное устройство подключается к Серверу администрирования и загружает общий сертификат. После установки сертификата на мобильное устройство это устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Если приложение Kaspersky Endpoint Security для Android уже установлено на устройство, пользователю нужно самостоятельно ввести параметры подключения к Серверу администрирования, получив их у администратора. После настройки параметров подключения мобильное устройство подключается к Серверу администрирования. Администратор выписывает общий сертификат для устройства и отправляет пользователю сообщение электронной почты или SMS с именем пользователя и паролем для загрузки сертификата. Пользователь загружает и устанавливает общий сертификат. После установки сертификата на мобильное устройство это устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли. Повторная загрузка и установка Kaspersky Endpoint Security для Android в этом случае не выполняются.

Подключение KES-устройств к Серверу администрирования

В зависимости от способа подключения устройств к Серверу администрирования существует две схемы развертывания Kaspersky Device Management для iOS для KES-устройств:

- схема развертывания с использованием прямого подключения устройств к Серверу администрирования;
- схема развертывания с использованием обратного прокси-сервера, поддерживающего Kerberos Constrained Delegation.

Прямое подключение устройств к Серверу администрирования

KES-устройства могут напрямую подключаться к порту 13292 Сервера администрирования.

В зависимости от способа аутентификации существуют два варианта подключения KES-устройств к Серверу администрирования:

- подключение устройств с использованием пользовательского сертификата;
- подключение устройств без пользовательского сертификата.

Подключение устройства с использованием пользовательского сертификата

При подключении устройства с использованием пользовательского сертификата происходит привязка этого устройства к учетной записи пользователя, для которой средствами Сервера администрирования назначен соответствующий сертификат.

В этом случае будет использована двусторонняя аутентификация SSL (mutual authentication). Как Сервер администрирования, так и устройство будут аутентифицированы с помощью сертификатов.

Подключение устройства без пользовательского сертификата

При подключении устройства без пользовательского сертификата оно не будет привязано ни к одной учетной записи пользователя на Сервере администрирования. Но при получении устройством любого сертификата будет произведена привязка этого устройства к пользователю, которому средствами Сервера администрирования назначен соответствующий сертификат.

При подключении устройства к Серверу администрирования будет использована односторонняя SSL-аутентификация (one-way SSL authentication), при которой только Сервер администрирования аутентифицируется с помощью сертификата. После получения устройством пользовательского сертификата тип аутентификации будет изменен на двустороннюю аутентификацию SSL (2-way SSL authentication, mutual authentication).

Схема подключения KES-устройств к Серверу с использованием принудительного делегирования Kerberos (KCD)

Схема подключения KES-устройств к Серверу администрирования с использованием Kerberos Constrained Delegation (KCD) предполагает:

- интеграция с обратным прокси-сервером, поддерживающим KCD;
- использование принудительного делегирования Kerberos Constrained Delegation (далее KCD) для аутентификации мобильных устройств;
- интеграцию с инфраструктурой открытых ключей (Public Key Infrastructure, далее PKI) для использования пользовательских сертификатов.

При использовании этой схемы подключения следует учесть следующее:

- Тип подключения KES-устройств к обратному прокси-серверу должен быть "two-way SSL authentication", то есть устройство должно подключаться к обратному прокси-серверу по своему пользовательскому сертификату. Для этого в инсталляционный пакет Kaspersky Endpoint Security для Android, который установлен на устройстве, необходимо интегрировать пользовательский сертификат. Этот KES-пакет должен быть создан Сервером администрирования специально для данного устройства (пользователя).
- Вместо серверного сертификата по умолчанию для мобильного протокола следует указать особый (кастомизированный) сертификат:

  1. В окне свойств Сервера администрирования в разделе **Параметры** установить флажок **Открыть порт для мобильных устройств** и в раскрывающемся списке выбрать **Добавить сертификат**.
  2. В открывшемся окне указать тот же сертификат, что задан на обратном прокси-сервере при публикации точки доступа к мобильному протоколу на Сервере администрирования.

- Пользовательские сертификаты для KES-устройств должны выписываться доменным Certificate Authority (CA). Следует учесть, если в домене несколько корневых CA, то пользовательские сертификаты должны быть выписаны тем CA, который прописан в публикации на обратном прокси-сервере.

  Обеспечить соответствие пользовательского сертификата заявленному выше требованию возможно несколькими способами:

  - Указать особый пользовательский сертификат в мастере создания инсталляционных пакетов и в мастере установки сертификатов.
  - Интегрировать Сервер администрирования с доменным PKI и настроить соответствующий параметр в правилах выписки сертификатов:

    1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Сертификаты**.
    2. В рабочей области папки **Сертификаты** по кнопке **Настроить правила выпуска сертификатов** откройте окно **Правила выпуска сертификатов**.
    3. В разделе **Интеграция с PKI** настройте интеграцию с инфраструктурой открытых ключей.
    4. В разделе **Выпуск мобильных сертификатов** укажите источник сертификатов.

Рассмотрим пример настройки ограниченного делегирования KCD со следующими допущениями:

- точка доступа к мобильному протоколу на Сервере администрирования поднята на 13292 порте;
- имя устройства с обратного прокси-сервера – firewall.mydom.local;
- имя устройства с Сервером администрирования – ksc.mydom.local;
- имя внешней публикации точки доступа к мобильному протоколу – kes4mob.mydom.global.

Доменная учетная запись для Сервера администрирования

Необходимо создать доменную учетную запись (например, KSCMobileSrvcUsr), под которой будет работать служба Сервера администрирования. Указать учетную запись для службы Сервера администрирования можно при установке Сервера администрирования или с помощью утилиты klsrvswch. Утилита klsrvswch расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Указать доменную учетную запись необходимо по следующим причинам:

- Функциональность по управлению KES-устройствами является неотъемлемой частью Сервера администрирования.
- Для правильной работы принудительного делегирования (KCD) принимающая сторона, которой является Сервер администрирования, должна работать под доменной учетной записью.

Service Principal Name для http/kes4mob.mydom.local

В домене под учетной записью KSCMobileSrvcUsr требуется прописать Service Principal Name (SPN) для публикации сервиса мобильного протокола на 13292 порту устройства с Сервером администрирования. Для устройства kes4mob.mydom.local с Сервером администрирования это будет выглядеть следующим образом:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

Настройка доменных свойств устройств с обратным прокси-сервером (firewall.mydom.local)

Для делегирования трафика нужно доверить устройство с обратным прокси-сервером (firewall.mydom.local) службе, определенной по SPN (http/kes4mob.mydom.local:13292).

Чтобы доверить устройство с обратным прокси-сервером службе, определенной по SPN (http/kes4mob.mydom.local:13292), администратору нужно выполнить следующие действия:

1. В оснастке Microsoft Management Console "Active Directory Users and Computers" выбрать устройство с установленным обратным прокси-сервером (firewall.mydom.local).
2. В свойствах устройства на вкладке **Delegation** для переключателя **Trust this computer for delegation to specified service only** выбрать вариант **Use any authentication protocol**.
3. В список **Services to which this account can present delegated credentials** добавить SPN http/kes4mob.mydom.local:13292.

Особый (кастомизированный) сертификат для публикации (kes4mob.mydom.global)

Для публикации мобильного протокола Сервера администрирования требуется выписать особый (кастомизированный) сертификат на FQDN kes4mob.mydom.global и указать его взамен серверного сертификата по умолчанию в параметрах мобильного протокола Сервера администрирования в Консоли администрирования. Для этого в окне свойств Сервера администрирования в разделе **Параметры** необходимо установить флажок **Открыть порт для мобильных устройств** и в раскрывающемся списке выбрать **Добавить сертификат**.

Следует учесть, что в контейнере с серверным сертификатом (файл с расширением p12 или pfx) должна также присутствовать цепочка корневых сертификатов (публичные части).

Настройка публикации на обратном прокси-сервере

На обратном прокси-сервере для трафика, идущего со стороны мобильного устройства на 13292 порт kes4mob.mydom.global, необходимо настроить KCD на SPN (http/kes4mob.mydom.local:13292) с использованием серверного сертификата, выписанного для FQND kes4mob.mydom.global. При этом следует учесть, что как на публикации, так и на публикуемой точке доступа (13292 порт Сервера администрирования) должен быть один и тот же серверный сертификат.

Использование Firebase Cloud Messaging

Для своевременной доставки команд на KES-устройства под управлением операционной системы Android в Kaspersky Security Center используется механизм push-нотификаций. Push-нотификации между KES-устройствами и Сервером администрирования осуществляются с помощью сервиса Firebase Cloud Messaging (далее – FCM). В Консоли администрирования Kaspersky Security Center вы можете указать параметры сервиса Cloud Messaging, чтобы подключить KES-устройства к этому сервису.

Для получения параметров Firebase Cloud Messaging вам необходимо иметь учетную запись Google.

Чтобы включить использование FCM:

1. В Консоли администрирования выберите узел **Управление мобильными устройствами** и папку **Мобильные устройства**.
2. В контекстном меню папки **Мобильные устройства** выберите пункт **Свойства**.
3. В окне свойств папки выберите раздел **Параметры Firebase Cloud Messaging**.
4. В поле **Номер проекта Firebase** укажите Sender ID FCM.
5. В поле **Файл приватного ключа (в формате JSON)** выберите файл приватного ключа.

   При следующей синхронизации с Сервером администрирования KES-устройства под управлением операционной системы Android будут подключены к службе Firebase Cloud Messaging.

Вы можете изменить параметры Firebase Cloud Messaging по кнопке **Сбросить параметры**.

При переключении на другой проект Firebase работа FCM возобновляется через 10 минут.

Сервис FCM работает на следующих диапазонах адресов:

- Со стороны KES-устройства необходим доступ на порты 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS), 5230 (HTTPS) следующих адресов:
  - google.com;
  - fcm.googleapis.com;
  - android.apis.google.com;
  - либо на все IP из списка "Google ASN 15169".
- Со стороны Сервера администрирования необходим доступ на порт 443 (HTTPS) следующих адресов:
  - fcm.googleapis.com;
  - либо на все IP из списка "Google ASN 15169".

В случае если в Консоли администрирования в свойствах Сервера администрирования заданы параметры прокси-сервера (**Дополнительно** / **Параметры доступа к сети Интернет**), то они будут использованы для взаимодействия с FCM.

При изменении значения `strDeviceRegId` устройства в таблице gcm_devices в серверной части FCM синхронизация измененного значения с серверной частью Kaspersky Security Center занимает 5 минут. Во время синхронизации сообщения могут поступать с задержкой на устройство, для которого было изменено значение `strDeviceRegId`.

Настройка FCM: получение Sender ID и файла закрытого ключа

Чтобы настроить FCM:

1. Зарегистрируйтесь на портале Google.
2. Перейдите в консоль Firebase.
3. Выполните одно из следующих действий:
   - Чтобы создать проект, нажмите на кнопку **Create a project** и следуйте инструкциям на экране.
   - Откройте существующий проект.
4. Нажмите на значок шестеренки и выберите **Project settings**.

   Откроется окно **Параметры проекта**.
5. Выберите вкладку **Cloud Messaging**.
6. Скопируйте Sender ID из поля **Sender ID** в разделе **Firebase Cloud Messaging API (V1)**.
7. Выберите вкладку **Service accounts** и нажмите на кнопку **Generate new private key**.
8. В открывшемся окне нажмите на кнопку **Generate key**, чтобы сгенерировать и загрузить файл приватного ключа.

Firebase Cloud Messaging настроен.

Интеграция с инфраструктурой открытых ключей

Интеграция с инфраструктурой открытых ключей (Public Key Infrastructure, далее PKI) в первую очередь предназначена для упрощения выпуска доменных пользовательских сертификатов Сервером администрирования.

Администратор может назначить для пользователя доменный сертификат в Консоли администрирования. Это можно сделать одним из следующих способов:

- назначить пользователю особый (кастомизированный) сертификат из файла в мастере установки сертификатов;
- выполнить интеграцию с PKI и назначить PKI источником сертификатов для конкретного типа сертификатов либо для всех типов сертификатов.

Параметры интеграции с PKI доступны в рабочей области папки **Управление мобильными устройствами** / **Сертификаты** при переходе по ссылке **Интегрировать с инфраструктурой открытых ключей**.

Общий принцип интеграции с PKI для выпуска доменных сертификатов пользователей

В Консоли администрирования по ссылке **Интегрировать с инфраструктурой открытых ключей** в рабочей области папки **Управление мобильными устройствами** / **Сертификаты** следует задать доменную учетную запись, которая будет использована Сервером администрирования для выписки доменных пользовательских сертификатов посредством доменного CA (далее – учетная запись, под которой производится интеграция с PKI).

Обратите внимание:

- В параметрах интеграции с PKI существует возможность указать шаблон по умолчанию для всех типов сертификатов. Тогда как в правилах выпуска сертификатов (правила доступны в рабочей области папки **Управление мобильными устройствами** / **Сертификаты** по кнопке **Настроить правила выпуска сертификатов**) присутствует возможность задать шаблон для каждого типа сертификата отдельно.
- На устройстве с установленным Сервером администрирования в хранилище сертификатов учетной записи, под которой производится интеграция с PKI, должен быть установлен специализированный сертификат Enrollment Agent (EA). Сертификат Enrollment Agent (EA) выписывает администратор доменного CA (Certificate Authority).

Учетная запись, под которой производится интеграция с PKI, должна соответствовать следующим критериям:

- Является доменным пользователем.
- Является локальным администратором устройства с установленным Сервером администрирования, с которого производится интеграция с PKI.
- Обладает правом *Вход в качестве службы*.
- Под этой учетной записью необходимо хотя бы один раз запустить устройство с установленным Сервером администрирования, чтобы создать постоянный профиль пользователя.

Веб-сервер Kaspersky Security Center

Веб-сервер Kaspersky Security Center (далее Веб-сервер) – это компонент Kaspersky Security Center. Веб-сервер предназначен для публикации автономных инсталляционных пакетов, автономных инсталляционных пакетов для мобильных устройств, iOS MDM-профилей, а также файлов из папки общего доступа.

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

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

Настройка Веб-сервера

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

Установка Kaspersky Security Center

В этом разделе описывается установка компонентов Kaspersky Security Center. Если вы хотите установить приложение локально только на одно устройство, доступны два варианта установки:

- **Стандартная**. Этот вариант рекомендуется, если вы хотите ознакомиться с приложением Kaspersky Security Center, например протестировать его работу на небольшом участке сети вашей организации. При стандартной установке вы настраиваете только параметры базы данных. Также вы можете установить только набор плагинов управления, заданный по умолчанию, для приложений "Лаборатории Касперского". Вы также можете воспользоваться стандартной установкой, если вы уже имеете опыт работы с Kaspersky Security Center и знаете, как после стандартной установки настроить все необходимые вам параметры.

- **Пользовательский**. Этот вариант рекомендуется, если вы планируете настроить параметры Kaspersky Security Center, такие как путь к папке общего доступа, учетные записи и порты подключения к Серверу администрирования, а также параметры базы данных. Выборочная установка позволяет указать, какие плагины управления приложениями "Лаборатории Касперского" будут установлены. При необходимости вы можете запустить выборочную установку в тихом режиме.

Если в сети установлен хотя бы один Сервер администрирования, Серверы на других устройствах сети могут быть установлены с помощью задачи удаленной установки методом принудительной установки. При создании задачи удаленной установки приложения необходимо использовать инсталляционный пакет Сервера администрирования: ksc_<version_number>.<build number>_full_<localization language>.exe.

Используйте этот пакет, если вы хотите установить все компоненты, необходимые для работы всех функций Kaspersky Security Center, или обновить существующие версии этих компонентов.

Если хотите развернуть отказоустойчивый кластер Kaspersky Security Center, вам необходимо установить Kaspersky Security Center на все узлы кластера.

Подготовка к установке

Выполните следующие действия перед запуском установки.

- **Проверка требований к оборудованию и программному обеспечению**

  Убедитесь, что аппаратное и программное обеспечение устройства соответствует требованиям, предъявляемым к Серверу администрирования и Консоли администрирования.

- **Выбор и установка системы управления базами данных (СУБД)**

  Kaspersky Security Center хранит свою информацию в базе данных, управляемой СУБД. Установите СУБД в сети до установки Kaspersky Security Center (узнайте больше о том, как выбрать СУБД). Если вы решили установить СУБД PostgreSQL или Postgres Pro, укажите пароль для суперпользователя. Если пароль не указан, Сервер администрирования может не подключиться к базе данных.

  Рекомендуется устанавливать Сервер администрирования на выделенный сервер, а не на контроллер домена. Если вы устанавливаете Kaspersky Security Center на сервер, выполняющий роль контроллера домена только для чтения (RODC), Microsoft SQL Server (SQL Express) не должен быть установлен локально (на этом же устройстве). В этом случае рекомендуется установить Microsoft SQL Server (SQL Express) удаленно (на другое устройство) или использовать MySQL, MariaDB или PostgreSQL, если вам нужно установить СУБД локально.

- **Подготовка папок для Сервера администрирования, Агента администрирования и Консоли администрирования**

  Сервер администрирования, Агент администрирования и Консоль администрирования должны быть установлены в папках, в которых выключен учет регистра. Также необходимо выключить учет регистра для общей папки Сервера администрирования и скрытой папки Kaspersky Security Center (%ALLUSERSPROFILE%\KasperskyLab\adminkit).

- **Удалите старую версию Агента администрирования**

  Вместе с компонентом Сервер администрирования на устройство будет установлена серверная версия Агента администрирования. Его совместная установка с обычной версией Агента администрирования невозможна. Если серверная версия Агента администрирования уже установлена на вашем устройстве, требуется удалить ее и запустить установку Сервера администрирования повторно. Подробнее о серверной версии Агента администрирования см. раздел Изменения в системе после установки Kaspersky Security Center.

- **Проверка учетных записей**

  Для установки Kaspersky Security Center необходимо наличие прав локального администратора на устройстве, где осуществляется установка.

  Kaspersky Security Center поддерживает управляемые учетные записи службы и групповые управляемые учетные записи службы. Если эти типы учетных записей используются в вашем домене и вы хотите указать одну из них в качестве учетной записи для службы Сервера администрирования, то сначала установите учетную запись на том же устройстве, на котором вы хотите установить Сервер администрирования. Подробнее об установке управляемых учетных записей служб на локальном устройстве см. в официальной документации Microsoft.

Учетные записи для работы с СУБД

Для установки Сервера администрирования и работы с ним вам потребуется учетная запись Windows, под которой вы будете запускать приложение установки Сервера администрирования (далее также "инсталлятор"), учетная запись Windows, под которой вы будете запускать службу Сервера администрирования, и внутренняя учетная запись СУБД для доступа к СУБД. Можно создать учетные записи или использовать существующие. Все эти учетные записи требуют определенных прав. Набор необходимых учетных записей и их права зависят от следующих критериев:

- Тип СУБД:
  - Microsoft SQL Server (с аутентификацией Windows или с аутентификацией SQL Server).
  - MySQL или MariaDB.
  - PostgreSQL или Postgres Pro.
- Расположение СУБД:
  - **Локальная СУБД**. *Локальной СУБД* называется СУБД, установленная на том же устройстве, что и Сервер администрирования;
  - **Удаленная СУБД**. *Удаленной СУБД* называется СУБД, установленная на другом устройстве.
- Способ создания базы данных Сервера администрирования:
  - **Автоматически**. При установке Сервера администрирования вы можете автоматически создать базу данных Сервера администрирования (далее также база данных Сервера) с помощью инсталлятора.
  - **Вручную**. Можно использовать приложение стороннего производителя (например, SQL Server Management Studio) или скрипт для создания пустой базы данных. После этого вы можете указать эту базу данных в качестве базы данных Сервера при установке Сервера администрирования.

При предоставлении прав и разрешений учетным записям соблюдайте принцип наименьших привилегий. Это означает, что предоставленных прав достаточно только для выполнения требуемых действий.

В приведенных ниже таблицах содержится информация о системных правах и правах на СУБД, которые требуется предоставить учетным записям перед установкой и запуском Сервера администрирования.

Microsoft SQL Server с аутентификацией Windows

Если вы выбираете SQL Server в качестве СУБД, можно использовать аутентификацию Windows для доступа к SQL Server. Настройте системные права для учетной записи Windows, используемой для запуска приложения установки, и для учетной записи Windows, используемой для запуска службы Сервера администрирования. В SQL Server создайте учетные записи для этих учетных записей Windows. В зависимости от метода создания базы данных Сервера предоставьте необходимые права SQL Server этим учетным записям, как описано в таблице ниже. Подробнее о настройке прав учетных записей см. раздел Настройка учетных записей для работы с SQL Server (аутентификация Windows).

СУБД: Microsoft SQL Server (в том числе и Express Edition) с аутентификацией Windows

	Автоматическое создание базы данных (приложением установки)	Создание базы данных вручную (администратором)
Учетная запись, от имени которой работает инсталлятор	• Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД. • Локальная СУБД: учетная запись локального администратора или учетная запись домена.	• Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД. • Локальная СУБД: учетная запись локального администратора или учетная запись домена.

Права учетной записи, от имени которой работает инсталлятор	• Системные права: права локального администратора.
	• Права SQL Server:
	  • Роль уровня сервера: sysadmin.
		• Системные права: права локального администратора.
		• Права SQL Server:
		  • Роль уровня сервера: public.
		  • Роль членства базы данных для базы данных Сервера: db_owner, public.
		  • Схема по умолчанию для базы данных Сервера: dbo.

Учетная запись службы Сервера администрирования	• Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД.
	• Локальная СУБД:
	  • Учетная запись Windows, выбранная администратором.
	  • Учетная запись в формате KL-AK-*, которую приложение установки создает автоматически.
		• Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД.
		• Локальная СУБД:
		  • Учетная запись Windows, выбранная администратором.
		  • Учетная запись в формате KL-AK-*, которую создает приложение установки автоматически (в этом случае не рекомендуется создавать учетную запись KL-AK-*).

Права учетной записи службы Сервера администрирования	• Системные права: необходимые права, присвоенные инсталлятором.
	• Права SQL Server: необходимые права, присвоенные инсталлятором.
		• Системные права: необходимые права, присвоенные инсталлятором.
		• Права SQL Server:
		  • Роль уровня сервера: public.
		  • Роль членства базы данных для базы данных Сервера: db_owner, public.
		  • Схема по умолчанию для базы данных Сервера: dbo.

Microsoft SQL Server с аутентификацией SQL Server

Если вы выбираете SQL Server в качестве СУБД, вы можете использовать аутентификацию SQL Server для подключения к SQL Server. Настройте системные права для учетной записи Windows, используемой для запуска приложения установки, и для учетной записи Windows, используемой для работы с Сервером администрирования. В SQL Server создайте учетную запись с паролем, чтобы использовать это для аутентификации. Затем предоставьте этой учетной записи SQL Server необходимые права, перечисленные в таблице ниже. Подробнее о настройке прав учетных записей см. раздел Настройка учетных записей для работы с SQL Server (аутентификация SQL Server).

СУБД: Microsoft SQL Server (в том числе и Express Edition) с аутентификацией SQL Server

	Автоматическое создание базы данных (приложением установки)	Создание базы данных вручную (администратором)
Учетная запись, от имени которой работает инсталлятор	• Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД. • Локальная СУБД: учетная запись локального администратора или учетная запись домена.	• Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД. • Локальная СУБД: учетная запись локального администратора или учетная запись домена.

	Автоматическое создание базы данных (приложением установки)	Создание базы данных вручную (администратором)
Права учетной записи, от имени которой работает инсталлятор	Системные права: права локального администратора.	Системные права: права локального администратора.

Учетная запись службы Сервера администрирования	• Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД.
	• Локальная СУБД:
	  • Учетная запись Windows, выбранная администратором.
	  • Учетная запись в формате KL-AK-*, которую приложение установки создает автоматически.
		• Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД.
		• Локальная СУБД:
		  • Учетная запись пользователя Windows, выбранная администратором.
		  • Учетная запись в формате KL-AK-*, которую приложение установки создает автоматически.

Права учетной записи службы Сервера администрирования	Системные права: необходимые права, присвоенные инсталлятором.	Системные права: необходимые права, присвоенные инсталлятором.

Права учетной записи, используемой для аутентификации SQL Server	Права SQL Server, необходимые для создания базы данных и установки Сервера администрирования:
	• Роль уровня сервера: public.
	• Роль членства базы данных для базы данных *master*: db_owner.
	• Схема по умолчанию для базы данных *master*: dbo.
	• Разрешения:
	  • CONNECT ANY DATABASE
	  • CONNECT SQL
	  • CREATE ANY DATABASE
	  • VIEW ANY DATABASE
	  • VIEW SERVER STATE (если включен параметр **Always On**)
	Права SQL Server, необходимые для работы с Сервером администрирования:
	• Роль уровня сервера: public.
	• Роль членства базы данных для базы данных Сервера: db_owner.
	• Схема по умолчанию для базы данных Сервера: dbo.
	• Разрешения:
	  • CONNECT SQL
	  • VIEW ANY DATABASE
	  • VIEW SERVER STATE (если включен параметр **Always On**)
	  • VIEW ANY DEFINITION
		Права SQL Server:
		• Роль уровня сервера: public.
		• Роль членства базы данных для базы данных Сервера: db_owner.
		• Схема по умолчанию для базы данных Сервера: dbo.
		• Разрешения:
		  • CONNECT SQL
		  • VIEW ANY DATABASE
		  • VIEW ANY DEFINITION

Настройка прав SQL Server для восстановления данных Сервера администрирования

Чтобы восстановить данные Сервера администрирования из резервной копии, запустите утилиту klbackup под учетной записью Windows, под которой был установлен Сервер администрирования. Перед запуском утилиты klbackup на SQL Server предоставьте права для входа в SQL Server, связанного с этой учетной записью Windows. Права SQL Server различаются в зависимости от версии Сервера администрирования. Для Сервера администрирования версии 14.2 и выше можно назначить серверную роль sysadmin или серверную роль dbcreator.

Права SQL Server для восстановления базы данных Сервера администрирования

Сервер администрирования версии 14.2 и выше	Другие версии Сервера администрирования

• Права SQL Server:
  • Роль уровня сервера: dbcreator.
• Разрешения:
  • VIEW ANY DEFINITION
Перед запуском утилиты klbackup укажите флаг сервера KLSRV_SKIP_ADJUSTING_DBMS_ACCESS. Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. Далее выполните следующую команду в командной строке:
`klscflag.exe -fset -pv klserver -n KLSRV_SKIP_ADJUSTING_DBMS_ACCESS -t d -v 1`	

MySQL и MariaDB

Если вы выбираете MySQL или MariaDB в качестве СУБД, создайте внутреннюю учетную запись СУБД и предоставьте этой учетной записи необходимые права, перечисленные в таблице ниже. Приложение установки и служба Сервера администрирования используют эту внутреннюю учетную запись СУБД для доступа к СУБД. Обратите внимание, что способ создания базы данных не влияет на набор необходимых прав. Подробнее о настройке прав учетной записи см. раздел Настройка учетных записей для работы с MySQL и MariaDB.

СУБД: MySQL и MariaDB

	Автоматическое или ручное создание базы данных
Учетная запись, от имени которой работает инсталлятор	• Удаленная СУБД: только доменная учетная запись удаленного устройства с установленной СУБД. • Локальная СУБД: учетная запись локального администратора или учетная запись домена.
Права учетной записи, от имени которой работает инсталлятор	Системные права: права локального администратора.

Учетная запись службы Сервера администрирования	• Удаленная СУБД: только доменная учетная запись удаленного устройства с установленной СУБД.
	• Локальная СУБД:
	  • Учетная запись Windows, выбранная администратором.
	  • Учетная запись в формате KL-AK-*, которую приложение установки создает автоматически.

Права учетной записи службы Сервера администрирования	Системные права: необходимые права, присвоенные инсталлятором.
Права внутренней учетной записи СУБД	Схема привилегий: • База данных Сервера администрирования: ALL (кроме GRANT OPTION). • Схемы системы (mysql и sys): SELECT, SHOW VIEW. • Хранимая процедура sys.table_exists: EXECUTE (если вы используете MariaDB 10.5 или более раннюю версию в качестве СУБД, вам не нужно предоставлять право EXECUTE). Глобальные привилегии для всех схем: PROCESS, SUPER.

Подробную информацию о том, как переместить данные из общего табличного пространства в табличное пространство file-per-table, см. статью Перенос данных из общего табличного пространства в табличное пространство file-per-table в СУБД MySQL и MariaDB.

Настройка прав на восстановление данных Сервера администрирования

Прав, которые вы предоставили для внутренней учетной записи СУБД, достаточно для восстановления данных Сервера администрирования из резервной копии. Чтобы начать восстановление, запустите утилиту klbackup под учетной записью Windows, под которой был установлен Сервер администрирования.

PostgreSQL или Postgres Pro.

Если вы выбираете PostgreSQL или Postgres Pro в качестве СУБД, вы можете использовать пользователя *Postgres* (роль Postgres по умолчанию) или создать роль Postgres (далее также роль) для доступа к СУБД. В зависимости от способа создания базы данных Сервера предоставьте необходимые права роли, как описано в таблице ниже. Подробнее о настройке прав роли см. раздел Настройка учетных записей для работы с PostgreSQL или Postgres Pro.

СУБД: PostgreSQL или Postgres Pro

	Автоматическое создание базы данных		Создание базы данных вручную
Учетная запись, от имени которой работает инсталлятор	• Удаленная СУБД: только доменная учетная запись удаленного устройства с установленной СУБД. • Локальная СУБД: учетная запись локального администратора или учетная запись домена.		• Удаленная СУБД: только доменная учетная запись удаленного устройства с установленной СУБД. • Локальная СУБД: учетная запись локального администратора или учетная запись домена.
Права учетной записи, от имени которой работает инсталлятор	Системные права: права локального администратора.		Системные права: права локального администратора.

Учетная запись службы Сервера администрирования	• Удаленная СУБД: только доменная учетная запись удаленного устройства с установленной СУБД.
	• Локальная СУБД:
	  • Учетная запись Windows, выбранная администратором.
	  • Учетная запись в формате KL-AK-*, которую приложение установки создает автоматически.
			• Удаленная СУБД: только доменная учетная запись удаленного устройства с установленной СУБД.
			• Локальная СУБД:
			  • Учетная запись Windows, выбранная администратором.
			  • Учетная запись в формате KL-AK-*, которую приложение установки создает автоматически.

Права учетной записи службы Сервера администрирования	Системные права: необходимые права, присвоенные инсталлятором.		Системные права: необходимые права, присвоенные инсталлятором.
Права роли Postgres	Пользователю *Postgres* не требуются дополнительные права.	Права для новой роли: `CREATEDB`.	Для новой роли: • Права доступа к базе данных Сервера администрирования: `ALL`. • Права доступа ко всем таблицам в общедоступной схеме: `ALL`. • Права доступа ко всем последовательностям в общедоступной схеме: `ALL`.

Настройка прав на восстановление данных Сервера администрирования

Чтобы восстановить данные Сервера администрирования из резервной копии, запустите утилиту klbackup под учетной записью Windows, под которой был установлен Сервер администрирования. Обратите внимание, что роль Postgres, используемая для доступа к СУБД, должна иметь права владельца на базу данных Сервера администрирования.

Настройка учетных записей для работы с SQL Server (аутентификация Windows)

Предварительные требования

Прежде чем назначать права учетным записям, выполните следующие действия:

1. Убедитесь, что вы входите в систему под учетной записью локального администратора.
2. Установите среду для работы с SQL Server.
3. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете устанавливать Сервер администрирования.
4. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете запускать службу Сервера администрирования.
5. В SQL Server создайте учетную запись для учетной записи Windows, используемой для запуска приложения установки Сервера администрирования (далее также "инсталлятор"). Также создайте учетную запись Windows, используемую для запуска службы Сервера администрирования.

Если вы используете SQL Server Management Studio, на странице **Общие** окна свойств входа выберите параметр **Аутентификация Windows**.

> Если вы хотите установить Сервер администрирования и SQL Server на устройства, расположенные в разных доменах Windows, обратите внимание, что эти домены должны иметь двусторонние отношения доверия, чтобы обеспечить корректную работу Сервера администрирования, включая выполнение задач и применение политик. Информацию о необходимых учетных записях для работы с различными СУБД и правах учетных записей см. в разделе Учетные записи для работы с СУБД.

Настройка учетных записей для установки Сервера администрирования (автоматическое создание базы данных Сервера администрирования)

Чтобы настроить учетные записи для установки Сервера администрирования:

1. В SQL Server назначьте роль sysadmin на уровне сервера для учетной записи Windows, которая используется для запуска приложения установки.
2. Войдите в систему под учетной записью Windows, используемой для запуска приложения установки.
3. Запустите приложение установки Сервера администрирования.

   Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.
4. Выберите выборочную установку Сервера администрирования.
5. Выберите Microsoft SQL Server как СУБД, в которой хранится база данных Сервера администрирования.

6. Выберите Режим аутентификации Microsoft Windows, чтобы установить соединение между Сервером администрирования и SQL Server с помощью учетной записи Windows.

7. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования.

   Можно выбрать учетную запись пользователя Windows, для которой вы ранее создали учетную запись SQL Server. Кроме того, вы можете автоматически создать учетную запись Windows в формате KL-AK-* с помощью приложения установки. В этом случае приложение установки автоматически создает для этой учетной записи учетную запись для SQL Server. Независимо от выбора учетной записи приложение установки назначает необходимые системные права и права SQL Server учетной записи службы Сервера администрирования.

После завершения установки создается база данных Сервера и все необходимые системные права и права SQL Server назначаются учетной записи службы Сервера администрирования. Сервер администрирования готов к работе.

Настройка учетных записей для установки Сервера администрирования (создание базы данных Сервера администрирования вручную)

Чтобы настроить учетные записи для установки Сервера администрирования:

1. На SQL Server создайте пустую базу данных. Эта база данных будет использоваться в качестве базы данных Сервера администрирования (далее также база данных Сервера).

2. Для обеих учетных записей SQL Server, созданных для учетных записей Windows, укажите общедоступную роль уровня сервера и настройте сопоставление с созданной базой данных:

   - Роль уровня сервера: public.
   - Роль членства базы данных: db_owner, public.
   - Схема по умолчанию: dbo.

3. Войдите в систему под учетной записью Windows, используемой для запуска приложения установки.

4. Запустите приложение установки Сервера администрирования.

   Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

5. Выберите выборочную установку Сервера администрирования.

6. Выберите Microsoft SQL Server как СУБД, в которой хранится база данных Сервера администрирования.

7. Укажите имя созданной базы данных в качестве имени базы данных Сервера администрирования.

8. Выберите Режим аутентификации Microsoft Windows, чтобы установить соединение между Сервером администрирования и SQL Server с помощью учетной записи Windows.

9. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования.

   Вы можете выбрать учетную запись пользователя Windows, для которой вы ранее создали учетную запись входа в SQL Server и настроили права входа.

Не рекомендуется автоматически создавать учетную запись Windows в формате KL-AK-*. В этом случае приложение установки создает учетную запись Windows, для которой вы не создали и не настроили учетную запись SQL Server. Сервер администрирования не может использовать эту учетную запись для запуска службы Сервера администрирования. Если необходимо создать учетную запись KL-AK-* Windows, не запускайте Консоль администрирования после установки. Вместо этого сделайте следующее:

1. Остановите службу kladminserver.
2. В SQL Server создайте учетную запись SQL Server для созданной учетной записи KL-AK-* Windows.
3. Предоставьте права этой учетной записи SQL Server и настройте сопоставление с созданной базой данных:
   - Роль уровня сервера: public.
   - Роль членства базы данных: db_owner, public.
   - Схема по умолчанию: dbo.
4. Перезапустите службу kladminserver, а затем запустите Консоль администрирования.

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

Настройка учетных записей для работы с SQL Server (аутентификация SQL Server)

Предварительные требования

Прежде чем назначать права учетным записям, выполните следующие действия:

1. Убедитесь, что вы входите в систему под учетной записью локального администратора.
2. Установите среду для работы с SQL Server.
3. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете устанавливать Сервер администрирования.
4. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете запускать службу Сервера администрирования.
5. В SQL Server включите режим аутентификации SQL Server.

   Если вы используете SQL Server Management Studio, в окне свойств SQL Server на странице **Безопасность** выберите параметр **SQL Server и режим аутентификации Windows**.

6. В SQL Server создайте учетную запись с паролем. Приложение установки Сервера администрирования (приложение установки) и служба Сервера администрирования используют эту учетную запись SQL Server для доступа к SQL Server.

   Если вы используете SQL Server Management Studio, на странице **Общие** окна свойств входа выберите параметр **Аутентификация SQL-сервера**.

Если вы хотите установить Сервер администрирования и SQL Server на устройства, расположенные в разных доменах Windows, обратите внимание, что эти домены должны иметь двусторонние отношения доверия, чтобы обеспечить корректную работу Сервера администрирования, включая выполнение задач и применение политик. Информацию о необходимых учетных записях для работы с различными СУБД и правах учетных записей см. в разделе Учетные записи для работы с СУБД.

Настройка учетных записей для установки Сервера администрирования (автоматическое создание базы данных Сервера администрирования)

Чтобы настроить учетные записи для установки Сервера администрирования:

1. В SQL Server сопоставьте учетную запись SQL Server с учетной записью по умолчанию в базе данных *master*. База данных *master* является шаблоном для базы данных Сервера администрирования (далее также база данных Сервера). База данных *master* используется для сопоставления до тех пор, пока приложение установки не создаст базу данных Сервера. Предоставьте следующие права и разрешения учетной записи SQL Server:

   - Роль уровня сервера: public.
   - Роль членства базы данных для базы данных *master*: db_owner.
   - Схема по умолчанию для базы данных *master*: dbo.
   - Разрешения:
     - CONNECT ANY DATABASE
     - CONNECT SQL
     - CREATE ANY DATABASE
     - VIEW ANY DATABASE
2. Войдите в систему под учетной записью Windows, используемой для запуска приложения установки.
3. Запустите приложение установки.

   Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.
4. Выберите выборочную установку Сервера администрирования.
5. Выберите Microsoft SQL Server как СУБД, в которой хранится база данных Сервера администрирования.
6. Укажите имя базы данных Сервера администрирования.

7. Выберите режим аутентификации SQL Server, чтобы установить соединение между Сервером администрирования и SQL Server с помощью созданной учетной записью SQL Server. Затем укажите данные учетной записи SQL Server.

8. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования.

   Вы можете выбрать существующую учетную запись пользователя Windows или создать учетную запись Windows в формате KL-AK-* с помощью приложения установки. Независимо от выбранной учетной записи приложение установки назначает необходимые системные права учетной записи службы Сервера администрирования.

После завершения установки создается база данных Сервера и все необходимые системные права назначаются учетной записи службы Сервера администрирования. Сервер администрирования готов к работе.

Вы можете отменить привязку к базе данных *master*, так как приложение установки создала базу данных Сервера и настроила сопоставление с этой базой данных при установке Сервера администрирования.

Так как для автоматического создания базы данных требуется больше разрешений, чем для ежедневной работы с Сервером администрирования, вы можете отозвать некоторые разрешения. На SQL Server выберите учетную запись SQL Server и предоставьте следующие права для работы с Сервером администрирования:

- Роль уровня сервера: public.
- Роль членства базы данных для базы данных Сервера: db_owner.
- Схема по умолчанию для базы данных Сервера: dbo.
- Разрешения:
  - CONNECT SQL
  - VIEW ANY DATABASE

Настройка учетных записей для установки Сервера администрирования (создание базы данных Сервера администрирования вручную)

Чтобы настроить учетные записи для установки Сервера администрирования:

1. На SQL Server создайте пустую базу данных. Эта база данных будет использоваться в качестве базы данных Сервера администрирования.

2. В SQL Server предоставьте следующие права и разрешения учетной записи SQL Server:

   - Роль уровня сервера: public.
   - Роль членства базы данных для создания базы данных: db_owner.
   - Схема по умолчанию для создания базы данных: dbo.

- Разрешения:
  - CONNECT SQL
  - VIEW ANY DATABASE

3. Войдите в систему под учетной записью Windows, используемой для запуска приложения установки.
4. Запустите приложение установки.

   Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.
5. Выберите выборочную установку Сервера администрирования.
6. Выберите Microsoft SQL Server как СУБД, в которой хранится база данных Сервера администрирования.
7. Укажите имя созданной базы данных в качестве имени базы данных Сервера администрирования.
8. Выберите режим аутентификации SQL Server, чтобы установить соединение между Сервером администрирования и SQL Server с помощью созданной учетной записью SQL Server. Затем укажите данные учетной записи SQL Server.
9. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования.

   Вы можете выбрать существующую учетную запись пользователя Windows или создать учетную запись Windows в формате KL-AK-* с помощью приложения установки. Независимо от выбранной учетной записи приложение установки назначает необходимые системные права учетной записи службы Сервера администрирования.

После завершения установки Сервер администрирования будет использовать созданную базу данных для хранения данных Сервера администрирования. Все необходимые системные права назначены учетной записи службы Сервера администрирования. Сервер администрирования готов к работе.

Настройка учетных записей для работы с MySQL и MariaDB

Предварительные требования

Прежде чем назначать права учетным записям, выполните следующие действия:

1. Убедитесь, что вы входите в систему под учетной записью локального администратора.
2. Установите среду для работы с MySQL или MariaDB.
3. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете устанавливать Сервер администрирования.
4. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете запускать службу Сервера администрирования.

Настройка учетных записей для установки Сервера администрирования

Чтобы настроить учетные записи для установки Сервера администрирования:

1. Запустите среду для работы с MySQL или MariaDB под учетной записью root, которую вы создали при установке СУБД.

2. Создайте внутреннюю учетную запись СУБД с паролем. Приложение установки Сервера администрирования (далее также приложение установки) и служба Сервера администрирования используют эту внутреннюю учетную запись СУБД для доступа к СУБД. Предоставьте этой учетной записи следующие права:

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

   Чтобы создать внутреннюю учетную запись СУБД и предоставить этой учетной записи необходимые права, запустите приведенный ниже скрипт (в этом скрипте учетная запись СУБД – *KSCAdmin*, а имя базы данных Сервера администрирования – *kav*):

   ```
   /* Создать пользователя с именем KSCAdmin */
   CREATE USER 'KSCAdmin'
   /* Указать пароль для KSCAdmin */
   IDENTIFIED BY '<пароль>';
   ```

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

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

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

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

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

   ```
   /* Предоставить привилегии KSCAdmin */
   GRANT USAGE ON *.* TO 'KSCAdmin';
   GRANT ALL ON kav.* TO 'KSCAdmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
   GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
   GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
   GRANT PROCESS ON *.* TO 'KSCAdmin';
   ```

```
GRANT SUPER ON *.* TO 'KSCAdmin';
```

> Если вы используете MariaDB 10.5 или более раннюю версию в качестве СУБД, вам не нужно предоставлять право EXECUTE. В этом случае исключите из скрипта следующую команду: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'`.

3. Чтобы просмотреть список привилегий, предоставленных учетной записи СУБД, запустите следующий скрипт:

   ```
   SHOW grants for 'KSCAdmin';
   ```

4. Чтобы вручную создать базу данных Сервера администрирования, запустите следующий скрипт (в этом скрипте имя базы данных Сервера администрирования – *kav*):

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET ascii
   DEFAULT COLLATE ascii_general_ci;
   ```

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

5. Войдите в систему под учетной записью Windows, используемой для запуска приложения установки.

6. Запустите приложение установки.

   Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

7. Выберите выборочную установку Сервера администрирования.

8. Выберите MySQL или MariaDB как СУБД, в которой хранится база данных Сервера администрирования.

9. Укажите имя базы данных Сервера администрирования. Используйте то же имя базы данных, которое вы указали в скрипте.

10. Укажите учетные данные учетной записи СУБД, которую вы создали с помощью скрипта.

11. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования.

    Вы можете выбрать существующую учетную запись пользователя Windows или автоматически создать учетную запись Windows в формате KL-AK-* с помощью приложения установки. Независимо от выбранной учетной записи приложение установки назначает необходимые системные права учетной записи службы Сервера администрирования.

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

Перенос данных из общего табличного пространства в табличное пространство file-per-table в СУБД MySQL или MariaDB

Для СУБД MySQL и MariaDB вы можете хранить данные следующими способами:

- В качестве общего табличного пространства, когда данные всех пользовательских баз данных хранятся в одном файле (обычно в файле `ibdata1`).
- В качестве табличного пространства file-per-table, когда для каждой таблицы создается отдельное пространство данных в виде отдельного файла.

Использование общего табличного пространства увеличивает риск фрагментации табличного пространства. Поскольку выполнить операцию `SHRINK` невозможно, файл в общем табличном пространстве может занимать около 90% дискового пространства. Это отрицательно сказывается на производительности дисковой подсистемы. Поэтому стоит выбрать табличное пространство file-per-table.

В этой статье описывается, как переместить данные из общего табличного пространства в табличное пространство file-per-table. Если СУБД MySQL или MariaDB также используются другими приложениями, вам необходимо переместить базы данных этих приложений в табличное пространство file-per-table.

> Рекомендуется выполнять перенос только в том случае, если вы используете СУБД MySQL или MariaDB для Сервера администрирования.
> Перемещение данных из общего табличного пространства в табличное пространство file-per-table может увеличить нагрузку на дисковую подсистему.

Предварительные требования

Перед тем как начать, убедитесь в следующем:

- Вы создали резервную копию данных Сервера администрирования, запустив либо задачу резервного копирования данных, либо утилиту klbackup.
- Вы создали резервную копию других приложений, базы данных которых управляются СУБД MySQL или MariaDB (если есть).
- На устройстве с установленной СУБД в разделе с базой данных есть свободное место на диске.

Требуемое дисковое пространство составляет 150% от текущего общего размера баз данных (текущего размера файла `ibdata1`).

Процесс

Чтобы переместить данные из общего табличного пространства в табличное пространство file-per-table:

1. Остановите службу Сервера администрирования Kaspersky Security Center и другие приложения, использующие экземпляр СУБД, для которого вы хотите выполнить эту процедуру.
2. В зависимости от версии СУБД войдите в свою СУБД как суперпользователь, а затем в любом приложении запустите скрипт `fix_tablespace.sql`.

   Вы можете просмотреть скрипты `fix_tablespace.sql`, перейдя по ссылкам:

Просмотреть скрипт для MySQL 5.7 и MariaDB 10.1+

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;

DELIMITER //

CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()

BEGIN

    DECLARE __st_FETCH_STATUS INT;

    DECLARE `schemaName` VARCHAR(192);

    DECLARE `tableName` VARCHAR(192);

    DECLARE `curIX` CURSOR FOR

    SELECT `TABLE_SCHEMA` , `TABLE_NAME`

    FROM information_schema.TABLES

    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;


    OPEN `curIX`;

    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;

    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO

        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );

        PREPARE stmt1 FROM @`strSQL`;

        EXECUTE stmt1;

        DEALLOCATE PREPARE stmt1;


        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;

    END WHILE;

    CLOSE `curIX`;

END

//

DELIMITER ;

SET GLOBAL innodb_file_per_table = 1;

CALL upgd_alter_all_tables_for_all_databases_to_innodb();

DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

Просмотреть скрипт для MySQL 8.0+

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;

DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;

    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
```

```
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;

        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
innodb_file_per_table;' );
        PREPARE stmt2 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt2;

        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;

SET GLOBAL innodb_file_per_table = 1;

CALL upgd_alter_all_tables_for_all_databases_to_innodb();

DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

Не останавливайте выполнение скрипта.
Если ошибок СУБД не было, но вы прервали выполнение скрипта, либо запустите скрипт повторно, либо прекратите выполнение шагов этой процедуры, перезагрузите службу СУБД и восстановите данные Сервера администрирования из резервной копии.

3. В разделе `[mysqld]` файла my.cnf установите для параметра `innodb_file_per_table` значение `1`.
4. Перезагрузите службу MySQL или MariaDB.
5. Запустите службу Сервера администрирования Kaspersky Security Center.

Данные будут перемещены из общего табличного пространства в табличное пространство file-per-table:

Настройка учетных записей для работы с PostgreSQL и Postgres Pro

Предварительные требования

Прежде чем назначать права учетным записям, выполните следующие действия:

1. Убедитесь, что вы входите в систему под учетной записью локального администратора.
2. Установите среду для работы с PostgreSQL и Postgres Pro.
3. Настройте сервер PostgreSQL или Postgres Pro для работы с Kaspersky Security Center 15.1.
4. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете устанавливать Сервер администрирования.
5. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете запускать службу Сервера администрирования.

Настройка учетных записей для установки Сервера администрирования (автоматическое создание базы данных Сервера администрирования)

Чтобы настроить учетные записи для установки Сервера администрирования:

1. Запустите среду для работы с PostgreSQL и Postgres Pro.
2. Выберите роль Postgres для доступа к СУБД. Вы можете использовать одну из следующих ролей:
   - Пользователь *Postgres* (роль Postgres по умолчанию).

     Если вы используете пользователя *Postgres*, предоставлять ему дополнительные права не требуется.
   - Новая роль Postgres.

     Если вы хотите использовать новую роль Postgres, создайте эту роль и предоставьте ей право CREATEDB. Для этого запустите следующий скрипт (в этом скрипте роль имеет значение *KSCAdmin*):

     ```
     CREATE USER "KSCAdmin" WITH PASSWORD '<password>' CREATEDB;
     ```

     Созданная роль будет использоваться в качестве владельца базы данных Сервера администрирования (далее также база данных Сервера).
3. Войдите в систему под учетной записью Windows, под которой было запущено приложение установки Сервера администрирования (далее также инсталлятор).
4. Запустите приложение установки.

   Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.
5. Выберите выборочную установку Сервера администрирования.
6. Выберите PostgreSQL или Postgres Pro как СУБД, в которой хранится база данных Сервера администрирования.
7. Укажите имя базы данных Сервера. Приложение установки автоматически создаст базу данных Сервера.
8. Укажите учетные данные роли Postgres.
9. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования.

   Вы можете выбрать существующую учетную запись пользователя Windows или автоматически создать учетную запись Windows в формате KL-AK-* с помощью приложения установки. Независимо от выбранной учетной записи приложение установки назначает необходимые системные права учетной записи службы Сервера администрирования.

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

Настройка учетных записей для установки Сервера администрирования (создание базы данных Сервера администрирования вручную)

Чтобы настроить учетные записи для установки Сервера администрирования:

1. Запустите среду для работы с Postgres.
2. Выполните вход под пользователем *Postgres* в базу данных *Postgres*.
3. Создайте роль Postgres (в этом примере роль – *KSCAdmin*):

```
CREATE USER "KSCAdmin" WITH PASSWORD '<password>';
```

4. Создайте базу данных Сервера администрирования (в этом примере имя базы данных Сервера администрирования – *KAV*):

```
CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
```

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

5. Предоставьте роли все права в базе данных Сервера администрирования.

```
GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
```

Убедитесь, что роль имеет привилегии по умолчанию CONNECT и TEMPORARY в базе данных Сервера администрирования.

6. Предоставьте следующие права созданной роли Postgres:

   - Права доступа ко всем таблицам в общедоступной схеме: ALL.
   - Права доступа ко всем последовательностям в общедоступной схеме: ALL.

   Для этого выполните вход под пользователем *Postgres* в базу данных Сервера и запустите следующий скрипт (в этом скрипте роль имеет значение *KSCAdmin*):

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
```

7. Войдите в систему под учетной записью Windows, используемой для запуска приложения установки.
8. Запустите приложение установки Сервера администрирования.

   Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

9. Выберите выборочную установку Сервера администрирования.

10. Выберите PostgreSQL или Postgres Pro как СУБД, в которой хранится база данных Сервера администрирования.

11. Укажите имя базы данных Сервера. Используйте то же имя базы данных, которое вы указали в скрипте. Учитывайте регистр при вводе имени базы данных.

12. Укажите учетные данные роли Postgres.

13. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования.

    Вы можете выбрать существующую учетную запись пользователя Windows или автоматически создать учетную запись Windows в формате KL-AK-* с помощью приложения установки. Независимо от выбранной учетной записи приложение установки назначает необходимые системные права учетной записи службы Сервера администрирования.

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

Сценарий: аутентификация Microsoft SQL Server

Информация в этом разделе применима только к конфигурациям, в которых Kaspersky Security Center использует Microsoft SQL Server в качестве системы управления базами данных.

Чтобы защитить данные Kaspersky Security Center, передаваемые в базу данных или из нее, а также данные, хранящиеся в базе данных, от несанкционированного доступа, вам нужно защитить связь между Kaspersky Security Center и SQL Server. Самый надежный способ обеспечить безопасную связь – это установить Kaspersky Security Center и SQL Server на одном устройстве и использовать механизм совместной памяти для обоих приложений. Во всех других случаях мы рекомендуем использовать сертификат SSL или TLS для аутентификации экземпляра SQL Server. Вы можете использовать сертификат доверенного центра сертификации (CA) или самоподписанный сертификат. Рекомендуется использовать сертификат доверенного центра сертификации, так как самоподписанный сертификат обеспечивает лишь ограниченную защиту.

Аутентификация SQL Server состоит из следующих этапов:

1. **Создание самоподписанного сертификата SSL или TLS для SQL Server в соответствии с требованиями сертификата**

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

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

   Например, чтобы создать TLS-сертификат, введите следующую команду в PowerShell:

   ```
   New-SelfSignedCertificate -DnsName SQL_HOST_NAME -CertStoreLocation cert:\LocalMachine
   -KeySpec KeyExchange
   ```

   В командной строке в качестве SQL_HOST_NAME вам нужно ввести имя экземпляра SQL Server, если экземпляр включен в домен, или ввести *полное доменное имя* (FQDN) экземпляра, если экземпляр не включен в домен. В мастере установки Сервера администрирования в качестве имени экземпляра SQL Server должно быть указано то же имя – имя экземпляра или полное доменное имя.

2. **Добавление сертификата на экземпляр SQL Server**

   Инструкции этого этапа зависят от платформы, на которой работает SQL Server. Дополнительную информацию см. в официальной документации:

   - Windows
   - Linux
   - Служба реляционных баз данных Amazon

   Чтобы использовать сертификат в отказоустойчивом кластере, необходимо установить сертификат на каждом узле отказоустойчивого кластера. Подробнее см. документацию Microsoft.

3. **Назначение разрешений для учетной записи службы**

   Убедитесь, что учетная запись службы, под которой запускается служба SQL Server, имеет разрешения "Полный доступ" для доступа к закрытым ключам. Подробнее см. документацию Microsoft.

4. **Добавление сертификата в список доверенных сертификатов для Kaspersky Security Center**

   На устройство Сервера администрирования добавьте сертификат в список доверенных сертификатов. Подробнее см. документацию Microsoft.

5. **Включение зашифрованных подключений между экземпляром SQL Server и Kaspersky Security Center**

   На устройстве Сервера администрирования установите значение `1` для переменной среды `KLDBADO_UseEncryption`. Например, в Windows Server 2012 R2 вы можете изменить переменные среды, нажав на **Переменные среды**, на вкладке **Дополнительно** окна **Свойства системы**. Добавьте переменную с именем `KLDBADO_UseEncryption` и установите значение `1`.

6. **Дополнительная настройка для использования TLS-протокола 1.2**

   Если вы используете TLS-протокол 1.2, дополнительно выполните следующие действия:

   - Убедитесь, что установленная версия SQL Server является 64-разрядным приложением.
   - Установите драйвер Microsoft OLE DB на устройство Сервера администрирования. Подробнее см. документацию Microsoft.
   - На устройстве Сервера администрирования установите значение `1` для переменной среды `KLDBADO_UseMSOLEDBSQL`. Например, в Windows Server 2012 R2 вы можете изменить переменные среды, нажав на **Переменные среды**, на вкладке **Дополнительно** окна **Свойства системы**. Добавьте новую переменную с именем `KLDBADO_UseMSOLEDBSQL` и установите значение `1`.

     Если версия драйвера OLE DB – 19 или выше, также установите значение `MSOLEDBSQL19` в переменную окружения `KLDBADO_ProviderName`.

7. **Включение использования протокола TCP/IP на именованном экземпляре SQL Server**

   Если вы используете именованный экземпляр SQL Server, дополнительно включите использование протокола TCP/IP и назначьте номер порта TCP/IP для компонента SQL Server Database Engine. При настройке подключения к SQL Server в мастере установки Сервера администрирования укажите имя экземпляра SQL Server и номер порта в поле **Имя экземпляра SQL Server**.

Сценарий: аутентификация MySQL Server

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

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

Включение односторонней SSL-аутентификации

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

1. **Создание самоподписанного TLS-сертификата для сервера MySQL.**

   Замените расположение в PowerShell на папку, где вы хотите хранить сертификаты. Выполните следующие команды:

```
$CertCA = New-SelfSignedCertificate `
-Subject "CN=CertCA" `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
-NotAfter (Get-Date).AddDays(365)

$CertCABase64 = [System.Convert]::ToBase64String($CertCA.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertLeaf = New-SelfSignedCertificate `
-Subject "CN=CertLeaf" `
-Signer $CertCA `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
-KeyExportPolicy Exportable `
-NotAfter (Get-Date).AddDays(365)

$CertLeafBase64 = [System.Convert]::ToBase64String($CertLeaf.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertLeafRSACng =
[System.Security.Cryptography.X509Certificates.RSACertificateExtensions]::GetRSAPrivateKey($CertLeaf)
$CertLeafKeyBytes =
$CertLeafRSACng.Key.Export([System.Security.Cryptography.CngKeyBlobFormat]::Pkcs8PrivateBlob)
$CertLeafKeyBase64 = [System.Convert]::ToBase64String($CertLeafKeyBytes,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertCAPemCert = @"
-----BEGIN CERTIFICATE-----
$CertCABase64
-----END CERTIFICATE-----
"@

$CertLeafPemKey = @"
-----BEGIN PRIVATE KEY-----
$CertLeafKeyBase64
-----END PRIVATE KEY-----
"@

$CertLeafPemCert = @"
-----BEGIN CERTIFICATE-----
$CertLeafBase64
-----END CERTIFICATE-----
"@

# Output to file

$CertCAPemCert | Out-File -FilePath ca-cert.pem -Encoding Ascii

$CertLeafPemKey | Out-File -FilePath server-key.pem -Encoding Ascii
$CertLeafPemCert | Out-File -FilePath server-cert.pem -Encoding Ascii
```

   Эти команды создают сертификаты для текущего пользователя и экспортируют сертификаты в формат PEM. Вам нужны только экспортированные файлы PEM для аутентификации Сервера. Чтобы удалить созданные сертификаты из Windows, выполните следующую команду в PowerShell:

```
certmgr.msc
```

   Найдите созданные сертификаты в папке **Личное** → **Сертификаты** и удалите их.

2. **Создайте файл флага сервера**

Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

С помощью утилиты klscflag создайте флаг сервера KLSRV_MYSQL_OPT_SSL_CA и укажите путь к сертификату в качестве его значения.

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

3. **Настройте базу данных**

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

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

Включение двусторонней SSL-аутентификации

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

1. **Создайте файлы флага сервера**

Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

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

```
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <путь к ca-cert.pem> -t s
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <путь к server-cert.pem> -t s
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <путь к server-key.pem> -t s
```

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

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

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

3. **Настройте базу данных**

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

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

Сценарий: аутентификация PostgreSQL Server

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

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

Аутентификация сервера PostgreSQL состоит из следующих этапов:

1. **Генерация сертификата для сервера PostgreSQL**

   В кроссплатформенной утилите на основе OpenSSL выполните следующие команды:

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

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

2. **Генерация сертификата для Сервера администрирования**

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

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

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

3. **Настройка аутентификации клиентского сертификата**

   Измените pg_hba.conf следующим образом:

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

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

4. **Задание сертификата PostgreSQL**

   Односторонняя SSL-аутентификация

   Измените postgresql.conf следующим образом (укажите правильный путь к файлам .crt и .key):

   ```
   listen_addresses ='localhost, server-ip'
   ```

   ```
   ssl = on
   ```

   ```
   ssl_cert_file = '<psql.crt>'
   ```

   ```
   ssl_key_file = '<psql.key>'
   ```

   Двусторонняя SSL-аутентификация

   Измените postgresql.conf следующим образом (укажите правильный путь к файлам .crt и .key):

   ```
   listen_addresses ='localhost, server-ip'
   ```

   ```
   ssl = on
   ```

   ```
   ssl_ca_file = '<postgres.crt>'
   ```

```
ssl_cert_file = '<psql.crt>'
ssl_key_file = '<psql.key>'
```

5. **Перезапуск демона PostgreSQL**

   Выполните следующую команду:

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

6. **Задание флага сервера для Сервера администрирования**

   Односторонняя SSL-аутентификация

   С помощью утилиты klscflag создайте флаг сервера KLSRV_POSTGRES_OPT_SSL_CA и укажите путь к сертификату в качестве его значения.

   Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Выполните следующую команду:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <путь к psql.crt> -t s
   ```

   Двусторонняя SSL-аутентификация

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

   Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Выполните следующие команды:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <путь к psql.crt> -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v <путь к postgres.crt> -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v <путь к postgres.key> -t s
   ```

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

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v <кодовая фраза> -t s
   ```

7. **Перезапуск службы Сервера администрирования**

Рекомендации по установке Сервера администрирования

В этом разделе содержатся рекомендации, касающиеся установки Сервера администрирования. В разделе также содержатся сценарии использования папки общего доступа на устройстве с Сервером администрирования для развертывания Агента администрирования на клиентских устройствах.

Создание учетных записей для служб Сервера администрирования на отказоустойчивом кластере

По умолчанию инсталлятор самостоятельно создает непривилегированные учетные записи для служб Сервера администрирования. Такое поведение наилучшим образом подходит для установки Сервера администрирования на обычное устройство.

Однако при установке Сервера администрирования на отказоустойчивый кластер следует поступить иначе:

1. Создать непривилегированные доменные учетные записи для служб Сервера администрирования и сделать их членами глобальной доменной группы безопасности KLAdmins.

2. Задать в инсталляторе Сервера администрирования созданные доменные учетные записи для служб.

Задание папки общего доступа

Во время установки Сервера администрирования можно задать месторасположение папки общего доступа. Также месторасположение папки общего доступа можно задать после установки, в свойствах Сервера администрирования. По умолчанию папка общего доступа создается на устройстве с Сервером администрирования (с доступом на чтение для встроенной группы **Everyone**). Однако в некоторых случаях (таких как высокая нагрузка или необходимость доступа из изолированной сети) целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

Папка общего доступа используется в нескольких сценариях развертывания Агента администрирования.

Учет регистра для общей папки должен быть выключен.

Удаленная установка средствами Сервера администрирования с помощью групповых политик Active Directory

В случае если устройства находятся в домене Windows (нет рабочих групп), первоначальное развертывание (установку Агента администрирования и приложения безопасности на пока еще не управляемые устройства) целесообразно выполнять при помощи групповых политик Active Directory. Развертывание выполняется с помощью штатной задачи удаленной инсталляции Kaspersky Security Center. Если размер сети велик, с целью уменьшения нагрузки на дисковую подсистему устройства с Сервером администрирования целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

Удаленная установка рассылкой UNC-пути на автономный пакет

В случае если пользователи устройств сети организации имеют права локального администратора, еще одним способом первоначального развертывания является создание автономного пакета Агента администрирования (или даже "спаренного" пакета Агента администрирования совместно с приложением безопасности). После создания автономного пакета нужно отправить пользователям устройств сети ссылку на пакет, находящийся в папке общего доступа. Установка запускается по ссылке.

Обновление из общей папки Сервера администрирования

В задаче обновления антивируса можно настроить обновление из папки общего доступа Сервера администрирования. Если задача назначена для большого количества устройств, целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

Установка образов операционных систем

Установка образов операционных систем всегда выполняется с использованием папки общего доступа: устройства читают из папки образы операционных систем. Если планируется развертывание образов на большом количестве устройств организации, то целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

Указание адреса Сервера администрирования

При установке Сервера администрирования можно задать адрес Сервера администрирования. Этот адрес по умолчанию используется при создании инсталляционных пакетов Агента администрирования.

В качестве адреса Сервера администрирования вы можете указать:

- NetBIOS-имя Сервера администрирования, указанное по умолчанию.
- Полное доменное имя (FQDN) Сервера администрирования, если система доменных имен (DNS) в сети организации настроена и работает должным образом.
- Внешний адрес, если Сервер администрирования установлен в демилитаризованной зоне (DMZ).

В дальнейшем адрес Сервера администрирования можно будет изменить средствами Консоли администрирования, однако при этом он не изменится автоматически в уже созданных инсталляционных пакетах Агента администрирования.

Стандартная установка

Стандартная установка – это установка Сервера администрирования, при которой используются заданные по умолчанию пути для файлов приложения, устанавливается набор плагинов по умолчанию и не включается Управление мобильными устройствами.

Чтобы установить Сервер администрирования Kaspersky Security Center на локальное устройство,

запустите исполняемый файл ksc_<номер версии>.<номер сборки>_full_<язык локализации>.exe.

Откроется окно с выбором приложений "Лаборатории Касперского" для установки. В окне с выбором приложений по ссылке **Установить Сервер администрирования Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге мастера установки требуется ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и Политикой конфиденциальности.

Вам также может быть предложено ознакомиться с Лицензионными соглашениями и Политиками конфиденциальности на доступные в дистрибутиве Kaspersky Security Center плагины для управления приложениями.

Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми условиями Лицензионного соглашения и Политики конфиденциальности, подтвердите это, установив соответствующие флажки.

Установка приложения будет продолжена после установки обоих флажков.

Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку приложения, нажав на кнопку **Отмена**.

Шаг 2. Выбор типа установки

В окне выбора типа установки укажите тип **Стандартная**.

Стандартная установка рекомендуется, если вы хотите ознакомиться с приложением Kaspersky Security Center, например, протестировать ее работу на небольшом участке вашей сети. При стандартной установке вы настраиваете только параметры базы данных. Параметры Сервера администрирования не настраиваются, для них используются заданные по умолчанию значения. Стандартная установка не позволяет выбрать устанавливаемые плагины управления, устанавливается заданный по умолчанию набор плагинов. Во время стандартной установки инсталляционные пакеты для мобильных устройств не создаются. Вы можете создать их позже в Консоли администрирования.

Шаг 3. Установка Kaspersky Security Center Web Console

Этот шаг отображается, только если вы используете 64-разрядную операционную систему. В противном случае этот шаг не отображается, поскольку Kaspersky Security Center Web Console не работает с 32-разрядными операционными системами.

По умолчанию будут установлены и Kaspersky Security Center Web Console, и Консоль администрирования на основе консоли Microsoft Management Console (MMC).

Если вы хотите установить только Kaspersky Security Center Web Console:

1. Выберите **Установить только одну из консолей**.
2. В раскрывающемся списке выберите **Консоль на основе веб-интерфейса**.

Установка Kaspersky Security Center Web Console запускается автоматически после завершения установки Сервера администрирования.

Если вы хотите установить только Консоль администрирования на основе консоли Microsoft Management Console (MMC):

1. Выберите **Установить только одну из консолей**.
2. В раскрывающемся списке выберите **Консоль на основе MMC**.

Шаг 4. Выбор размера сети

Укажите размер сети, в которой устанавливается Kaspersky Security Center. В зависимости от количества устройств в сети мастер настраивает параметры установки и отображение интерфейса приложения.

В таблице ниже перечислены параметры установки приложения и отображения интерфейса при выборе разных размеров сети.

Зависимость параметров установки от выбора размеров сети

Параметры	1–100 управляемых устройств	101–1000 управляемых устройств	1001–5000 управляемых устройств	Более 5000 управляемых устройств
Отображение в дереве консоли узла подчиненных и виртуальных Серверов администрирования и всех параметров, связанных с подчиненными и виртуальными Серверами (только в Консоли администрирования на базе MMC)	Отсутствует	Отсутствует	Присутствует	Присутствует
Отображение с разделами **Безопасность** в окнах свойств Сервера администрирования и групп администрирования (доступно только в Консоли администрирования на базе MMC)	Отсутствует	Отсутствует	Присутствует	Присутствует
Распределение времени запуска задачи обновления на клиентских устройствах случайным образом	Отсутствует	в интервале 5 минут	в интервале 10 минут	в интервале 10 минут

При подключении Сервера администрирования к серверу базы данных MySQL 5.7 или SQL Express не рекомендуется использовать приложение для управления более чем 10 000 устройств. Для системы управления базами данных MariaDB максимальное рекомендуемое количество управляемых устройств составляет 20 000.

Шаг 5. Выбор базы данных

На этом шаге мастера выберите одну из следующих систем управления базами данных (СУБД), которая будет использоваться для хранения базы данных Сервера администрирования:

- **Microsoft SQL Server или SQL Server Express**
- **MySQL или MariaDB**
- **PostgreSQL или Postgres Pro**

Рекомендуется устанавливать Сервер администрирования на выделенный сервер, а не на контроллер домена. Если вы устанавливаете Kaspersky Security Center на сервер, выполняющий роль контроллера домена только для чтения (RODC), Microsoft SQL Server (SQL Express) не должен быть установлен локально (на этом же устройстве). В этом случае рекомендуется установить Microsoft SQL Server (SQL Express) удаленно (на другое устройство) или использовать MySQL, MariaDB или PostgreSQL, если вам нужно установить СУБД локально.

Структура базы данных Сервера администрирования представлена в файле klakdb.chm, который находится в папке установки Kaspersky Security Center. Этот файл также доступен в архиве на портале "Лаборатории Касперского": klakdb.zip.

Шаг 6. Настройка параметров SQL-сервера

На этом шаге мастера укажите следующие параметры подключения в зависимости от выбранной вами системы управления базами данных (СУБД):

- Если вы выбрали **Microsoft SQL Server или SQL Server Express** на предыдущем шаге:
  - В поле **Имя экземпляра SQL-сервера** укажите имя SQL-сервера, установленного в сети. При помощи кнопки **Обзор** вы можете открыть список всех SQL-серверов, установленных в сети. По умолчанию поле не заполнено.

    Если вы подключаетесь к SQL Server через пользовательский порт, то вместе с именем экземпляра SQL Server укажите через запятую номер порта, например:

    ```
    SQL_Server_host_name,1433
    ```

    Если вы защищаете соединение между Сервером администрирования и SQL Server с помощью сертификата, укажите в поле **Имя экземпляра SQL-сервера** то же имя экземпляра, которое использовалось при создании сертификата. Если вы используете именованный экземпляр SQL Server, вместе с именем экземпляра SQL Server укажите через запятую номер порта, например:

    ```
    SQL_Server_name,1433
    ```

    Если вы используете несколько экземпляров SQL Server на одном устройстве, дополнительно укажите через обратную косую черту имя экземпляра, например:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

Если для SQL Server в корпоративной сети включена функция Always On, укажите имя прослушивателя группы доступности в поле **Имя экземпляра SQL-сервера**. Обратите внимание, что Сервер администрирования поддерживает только режим доступности с синхронной фиксацией, когда включена функция Always On.

- В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

Если на этом шаге вы хотите установить SQL-сервер на то устройство, с которого производите установку Kaspersky Security Center, нужно прервать установку и запустить ее снова после установки SQL-сервера. Поддерживаемые версии SQL Server перечислены в требованиях к системе.

Если вы хотите установить SQL-сервер на удаленное устройство, прерывать работу мастера установки Kaspersky Security Center не требуется. Установите SQL Server и вернитесь к установке Kaspersky Security Center.

- Если вы выбрали **MySQL или MariaDB** на предыдущем шаге:
  - В поле **Имя экземпляра SQL-сервера** укажите имя экземпляра СУБД. По умолчанию используется IP-адрес устройства, на которое устанавливается Kaspersky Security Center.
  - В поле **Порт** укажите порт для подключения Сервера администрирования к СУБД. По умолчанию установлен порт 3306.
  - В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.
- Если вы выбрали **PostgreSQL или Postgres Pro** на предыдущем шаге:
  - В поле **PostgreSQL или Postgres Pro Server** укажите имя экземпляра СУБД. По умолчанию используется IP-адрес устройства, на которое устанавливается Kaspersky Security Center.
  - В поле **Порт** укажите порт для подключения Сервера администрирования к СУБД. По умолчанию установлен порт 5432.
  - В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

Шаг 7. Выбор режима аутентификации

Определите режим аутентификации, который будет использоваться при подключении Сервера администрирования к системе управления базами данных (СУБД).

В зависимости от выбранной СУБД вы можете выбрать следующие режимы аутентификации:

- Для SQL Express или Microsoft SQL Server выберите один из следующих вариантов:
  - **Режим аутентификации Microsoft Windows**. В этом случае при проверке прав будет использоваться учетная запись для запуска Сервера администрирования.
  - **Режим аутентификации SQL-сервера**. В случае выбора этого варианта для проверки прав будет использоваться указанная в окне учетная запись. Заполните поля **Учетная запись** и **Пароль**.

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

Приложение проверяет, доступна ли база данных для обоих режимов аутентификации. Если база данных недоступна, отображается сообщение об ошибке и вам нужно указать правильные учетные данные.

Если база данных Сервера администрирования находится на другом устройстве и учетная запись Сервера администрирования не имеет доступа к серверу базы данных, то при установке или обновлении Сервера администрирования следует использовать режим аутентификации SQL-сервера. Это может происходить в случае, когда устройство с базой данных находится не в домене, или Сервер администрирования установлен под учетной записью LocalSystem.

- Для MySQL, MariaDB, PostgreSQL или Postgres Pro укажите учетную запись и пароль.

Шаг 8. Распаковка и установка файлов на жесткий диск

По окончании настройки параметров установки компонентов Kaspersky Security Center вы можете запустить установку файлов на жесткий диск.

Если для запуска установки требуются дополнительные приложения, мастер установки сообщит об этом перед началом установки Kaspersky Security Center в окне **Установка обязательных компонентов**. Необходимые приложения будут установлены автоматически после нажатия на кнопку **Далее**.

На последней странице можно выбрать, какую консоль требуется запустить для работы с Kaspersky Security Center:

- **Запустить Консоль на основе MMC**
- **Запустить как Kaspersky Security Center Web Console**

  Этот параметр доступен, только если на одном из предыдущих шагов вы выбрали установку Kaspersky Security Center Web Console.

Вы можете завершить работу мастера без запуска Kaspersky Security Center. Для этого нажмите на кнопку **Завершить**. Работу с Kaspersky Security Center можно начать позже в любое время.

При первом запуске Консоли администрирования или Kaspersky Security Center Web Console вы можете выполнить первоначальную настройку приложения.

По окончании работы мастера установки следующие компоненты приложения будут установлены на жесткий диск, на котором установлена операционная система:

- Сервер администрирования (совместно с серверной версией Агента администрирования);
- Консоль администрирования на основе консоли управления Microsoft Management Console (MMC);
- Kaspersky Security Center Web Console (если выбрана ее установка);
- доступные в дистрибутиве плагины управления приложениями.

Кроме того, будет установлено приложение Microsoft Windows Installer версии 4.5, если это приложение не было установлено ранее.

Выборочная установка

Выборочная установка – это установка Сервера администрирования, при которой вам предлагается выбрать компоненты для установки и указать папку, в которую будет установлено приложение.

С помощью этого типа установки вы можете настроить параметры базы данных, параметры Сервера администрирования, установить компоненты, которые не включены в стандартную установку и плагины управления приложениями безопасности "Лаборатории Касперского". Вы можете также включить Управление мобильными устройствами.

Чтобы установить Сервер администрирования Kaspersky Security Center на локальное устройство,

запустите исполняемый файл ksc_<номер версии>.<номер сборки>_full_<язык локализации>.exe.

Откроется окно с выбором приложений "Лаборатории Касперского" для установки. В окне с выбором приложений по ссылке **Установить Сервер администрирования Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге мастера установки требуется ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и Политикой конфиденциальности.

Вам также может быть предложено ознакомиться с Лицензионными соглашениями и Политиками конфиденциальности на доступные в дистрибутиве Kaspersky Security Center плагины для управления приложениями.

Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми условиями Лицензионного соглашения и Политики конфиденциальности, подтвердите это, установив соответствующие флажки.

Установка приложения будет продолжена после установки обоих флажков.

Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку приложения, нажав на кнопку **Отмена**.

Шаг 2. Выбор типа установки

В окне выбора типа установки укажите тип **Выборочная**.

Выборочная установка позволяет настроить параметры Kaspersky Security Center, такие как путь к папке общего доступа, учетные записи и порты подключения к Серверу администрирования, и параметры базы данных. Выборочная установка позволяет указать, какие плагины управления приложениями "Лаборатории Касперского" будут установлены. При выборочной установке вы можете создать инсталляционные пакеты для мобильных устройств, указав соответствующий параметр.

Шаг 3. Выбор компонентов для установки

Выберите компоненты Сервера администрирования Kaspersky Security Center, которые вы хотите установить:

- **Управление мобильными устройствами**. Установите этот флажок, если требуется создать инсталляционные пакеты для мобильных устройств во время работы мастера установки Kaspersky Security Center. Вы можете также создать инсталляционные пакеты для мобильных устройств вручную, после установки Сервера администрирования средствами Консоли администрирования.

- **Агент SNMP**. Получает статистическую информацию для Сервера администрирования по протоколу SNMP. Компонент доступен при установке приложения на устройство с установленным компонентом SNMP.

  После установки Kaspersky Security Center необходимые для получения статистической информации mib-файлы будут расположены в папке установки приложения во вложенной папке SNMP.

Компоненты Агент администрирования и Консоль администрирования не отображаются в списке компонентов. Эти компоненты устанавливаются автоматически, их установку отменить невозможно.

На этом шаге мастера также следует указать папку для установки компонентов Сервера администрирования. По умолчанию компоненты устанавливаются в папку <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Если папки с таким названием нет, она будет создана автоматически в процессе установки. Вы можете изменить папку назначения с помощью кнопки **Обзор**.

Шаг 4. Установка Kaspersky Security Center Web Console

Этот шаг отображается, только если вы используете 64-разрядную операционную систему. В противном случае этот шаг не отображается, поскольку Kaspersky Security Center Web Console не работает с 32-разрядными операционными системами.

По умолчанию будут установлены и Kaspersky Security Center Web Console, и Консоль администрирования на основе консоли Microsoft Management Console (MMC).

Если вы хотите установить только Kaspersky Security Center Web Console:

1. Выберите **Установить только одну из консолей**.

2. В раскрывающемся списке выберите **Консоль на основе веб-интерфейса**.

Установка Kaspersky Security Center Web Console запускается автоматически после завершения установки Сервера администрирования.

Если вы хотите установить только Консоль администрирования на основе консоли Microsoft Management Console (MMC):

1. Выберите **Установить только одну из консолей**.

2. В раскрывающемся списке выберите **Консоль на основе MMC**.

Шаг 5. Выбор размера сети

Укажите размер сети, в которой устанавливается Kaspersky Security Center. В зависимости от количества устройств в сети мастер настраивает параметры установки и отображение интерфейса приложения.

В таблице ниже перечислены параметры установки приложения и отображения интерфейса при выборе разных размеров сети.

Зависимость параметров установки от выбора размеров сети

Параметры	1–100 управляемых устройств	101–1000 управляемых устройств	1001–5000 управляемых устройств	Более 5000 управляемых устройств
Отображение в дереве консоли узла подчиненных и виртуальных Серверов администрирования и всех параметров, связанных с подчиненными и виртуальными Серверами (только в Консоли администрирования на базе MMC)	Отсутствует	Отсутствует	Присутствует	Присутствует
Отображение с разделами **Безопасность** в окнах свойств Сервера администрирования и групп администрирования (доступно только в Консоли администрирования на базе MMC)	Отсутствует	Отсутствует	Присутствует	Присутствует
Распределение времени запуска задачи обновления на клиентских устройствах случайным образом	Отсутствует	в интервале 5 минут	в интервале 10 минут	в интервале 10 минут

При подключении Сервера администрирования к серверу базы данных MySQL 5.7 или SQL Express не рекомендуется использовать приложение для управления более чем 10 000 устройств. Для системы управления базами данных MariaDB максимальное рекомендуемое количество управляемых устройств составляет 20 000.

Шаг 6. Выбор базы данных

На этом шаге мастера выберите одну из следующих систем управления базами данных (СУБД), которая будет использоваться для хранения базы данных Сервера администрирования:

- **Microsoft SQL Server или SQL Server Express**
- **MySQL или MariaDB**
- **PostgreSQL или Postgres Pro**

Рекомендуется устанавливать Сервер администрирования на выделенный сервер, а не на контроллер домена. Если вы устанавливаете Kaspersky Security Center на сервер, выполняющий роль контроллера домена только для чтения (RODC), Microsoft SQL Server (SQL Express) не должен быть установлен локально (на этом же устройстве). В этом случае рекомендуется установить Microsoft SQL Server (SQL Express) удаленно (на другое устройство) или использовать MySQL, MariaDB или PostgreSQL, если вам нужно установить СУБД локально.

Структура базы данных Сервера администрирования представлена в файле klakdb.chm, который находится в папке установки Kaspersky Security Center. Этот файл также доступен в архиве на портале "Лаборатории Касперского": klakdb.zip.

Шаг 7. Настройка параметров SQL-сервера

На этом шаге мастера укажите следующие параметры подключения в зависимости от выбранной вами системы управления базами данных (СУБД):

- Если вы выбрали **Microsoft SQL Server или SQL Server Express** на предыдущем шаге:
  - В поле **Имя экземпляра SQL-сервера** укажите имя SQL-сервера, установленного в сети. При помощи кнопки **Обзор** вы можете открыть список всех SQL-серверов, установленных в сети. По умолчанию поле не заполнено.

    Если вы подключаетесь к SQL Server через пользовательский порт, то вместе с именем экземпляра SQL Server укажите через запятую номер порта, например:

    ```
    SQL_Server_host_name,1433
    ```

    Если вы защищаете соединение между Сервером администрирования и SQL Server с помощью сертификата, укажите в поле **Имя экземпляра SQL-сервера** то же имя экземпляра, которое использовалось при создании сертификата. Если вы используете именованный экземпляр SQL Server, вместе с именем экземпляра SQL Server укажите через запятую номер порта, например:

    ```
    SQL_Server_name,1433
    ```

    Если вы используете несколько экземпляров SQL Server на одном устройстве, дополнительно укажите через обратную косую черту имя экземпляра, например:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

Если для SQL Server в корпоративной сети включена функция Always On, укажите имя прослушивателя группы доступности в поле **Имя экземпляра SQL-сервера**. Обратите внимание, что Сервер администрирования поддерживает только режим доступности с синхронной фиксацией, когда включена функция Always On.

- В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

Если на этом шаге вы хотите установить SQL-сервер на то устройство, с которого производите установку Kaspersky Security Center, нужно прервать установку и запустить ее снова после установки SQL-сервера. Поддерживаемые версии SQL Server перечислены в требованиях к системе.

Если вы хотите установить SQL-сервер на удаленное устройство, прерывать работу мастера установки Kaspersky Security Center не требуется. Установите SQL Server и вернитесь к установке Kaspersky Security Center.

- Если вы выбрали **MySQL или MariaDB** на предыдущем шаге:
  - В поле **Имя экземпляра SQL-сервера** укажите имя экземпляра СУБД. По умолчанию используется IP-адрес устройства, на которое устанавливается Kaspersky Security Center.
  - В поле **Порт** укажите порт для подключения Сервера администрирования к СУБД. По умолчанию установлен порт 3306.
  - В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.
- Если вы выбрали **PostgreSQL или Postgres Pro** на предыдущем шаге:
  - В поле **PostgreSQL или Postgres Pro Server** укажите имя экземпляра СУБД. По умолчанию используется IP-адрес устройства, на которое устанавливается Kaspersky Security Center.
  - В поле **Порт** укажите порт для подключения Сервера администрирования к СУБД. По умолчанию установлен порт 5432.
  - В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

Шаг 8. Выбор режима аутентификации

Определите режим аутентификации, который будет использоваться при подключении Сервера администрирования к системе управления базами данных (СУБД).

В зависимости от выбранной СУБД вы можете выбрать следующие режимы аутентификации:

- Для SQL Express или Microsoft SQL Server выберите один из следующих вариантов:
  - **Режим аутентификации Microsoft Windows**. В этом случае при проверке прав будет использоваться учетная запись для запуска Сервера администрирования.
  - **Режим аутентификации SQL-сервера**. В случае выбора этого варианта для проверки прав будет использоваться указанная в окне учетная запись. Заполните поля **Учетная запись** и **Пароль**.

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

Приложение проверяет, доступна ли база данных для обоих режимов аутентификации. Если база данных недоступна, отображается сообщение об ошибке и вам нужно указать правильные учетные данные.

Если база данных Сервера администрирования находится на другом устройстве и учетная запись Сервера администрирования не имеет доступа к серверу базы данных, то при установке или обновлении Сервера администрирования следует использовать режим аутентификации SQL-сервера. Это может происходить в случае, когда устройство с базой данных находится не в домене, или Сервер администрирования установлен под учетной записью LocalSystem.

- Для MySQL, MariaDB, PostgreSQL или Postgres Pro укажите учетную запись и пароль.

Шаг 9. Выбор учетной записи для запуска Сервера администрирования

Выберите учетную запись, под которой Сервер администрирования будет запускаться как служба.

- **Создать учетную запись автоматически**. Приложение создает локальную учетную запись KL-AK-*, под которой будет запускаться служба Сервера администрирования kladminserver.

  Вы можете выбрать этот вариант, если вы планируете разместить папку общего доступа и СУБД на том же устройстве, что и Сервер администрирования.

- **Выбрать учетную запись**. Служба Сервера администрирования (kladminserver) будет запускаться под выбранной вами учетной записью.

  Вам потребуется выбрать доменную учетную запись, например, если вы планируете использовать в качестве СУБД SQL-сервер любого выпуска, в том числе SQL-express, расположенный на другом устройстве, и/или если вы планируете разместить папку общего доступа на другом устройстве.

  Kaspersky Security Center поддерживает управляемые учетные записи службы (MSA) и групповые управляемые учетные записи службы (gMSA). Если такие учетные записи используются в вашем домене, вы можете выбрать одну из них в качестве учетной записи для службы Сервера администрирования.

  Прежде чем выбрать MSA или gMSA, необходимо установить учетную запись на том же устройстве, на котором вы хотите установить Сервер администрирования. Если учетная запись еще не установлена, отмените установку Сервера администрирования, установите учетную запись и перезапустите установку Сервера администрирования. Подробнее об установке управляемых учетных записей служб на локальном устройстве см. в официальной документации Microsoft.

  Чтобы указать MSA или gMSA:

  1. Нажмите на кнопку **Обзор**.
  2. В появившемся окне нажмите на кнопку **Object type**.
  3. Выберите тип **Учетная запись для служб** и нажмите на кнопку **OK**.
  4. Выберите нужную учетную запись и нажмите на кнопку **OK**.

Выбранная вами учетная запись должна обладать различными правами в зависимости от того, какую СУБД вы планируете использовать.

Из соображений безопасности не делайте учетную запись, под которой запускается Сервер администрирования, привилегированной.

Учетную запись Сервера администрирования изменить позже невозможно. Для использования другой учетной записи Сервера администрирования нужно переустановить отказоустойчивый кластер.

Шаг 10. Выбор учетной записи для запуска служб Kaspersky Security Center

Выберите учетную запись, под которой будут запускаться службы Kaspersky Security Center на этом устройстве:

- **Создать учетную запись автоматически**. Kaspersky Security Center создает локальную учетную запись KlScSvc на этом устройстве в группе kladmins. Службы Kaspersky Security Center будут запускаться под созданной учетной записью.

- **Выбрать учетную запись**. Службы Kaspersky Security Center будут запускаться под выбранной вами учетной записью.

  Вам потребуется выбрать доменную учетную запись, например, если вы планируете сохранять отчеты в папке, расположенной на другом устройстве, или же если этого требует политика безопасности в вашей организации. Также вам может потребоваться выбрать доменную учетную запись при установке Сервера администрирования на отказоустойчивый кластер.

Из соображений безопасности не делайте учетную запись, под которой запускаются службы, привилегированной.

Под выбранной учетной записью будут запускаться службы прокси-сервера KSN (ksnproxy), прокси-сервера активации "Лаборатории Касперского" (klactprx) и портала авторизации "Лаборатории Касперского" (klwebsrv).

Шаг 11. Определение папки общего доступа

Определите место размещения и название папки общего доступа, которая будет использоваться для следующих целей:

- хранения файлов, необходимых для удаленной установки приложений (файлы копируются на Сервер администрирования при создании инсталляционных пакетов);

- размещения обновлений, копируемых с источника обновлений на Сервер администрирования.

К этому ресурсу будет открыт общий доступ на чтение для всех пользователей.

Вы можете выбрать один из двух вариантов:

- **Создать папку общего доступа**. Создание новой папки. Укажите путь к папке в расположенном ниже поле.

- **Выбрать существующую папку общего доступа**. Выбор папки общего доступа из числа уже существующих.

Папка общего доступа может размещаться как локально на устройстве, с которого производится установка, так и удаленно, на любом из клиентских устройств, входящих в состав сети организации. Вы можете указать папку общего доступа с помощью кнопки **Обзор** или вручную, введя в соответствующем поле UNC-путь (например, \\server\Share).

По умолчанию создается локальная папка KLSHARE в папке, заданной для установки компонентов Kaspersky Security Center.

Вы можете определить общую папку позже, если нужно.

Шаг 12. Настройка параметров подключения к Серверу администрирования

Настройте параметры подключения к Серверу администрирования:

- **Порт**

  Номер порта, по которому выполняется подключение к Серверу администрирования.

  По умолчанию установлен порт 14000.

- **SSL-порт**

  Номер SSL-порта, по которому осуществляется защищенное подключение к Серверу администрирования с использованием протокола SSL.

  По умолчанию установлен порт 13000.

- **Длина ключа шифрования**

  Выберите длину ключа шифрования: 1024 бита или 2048 бит.

  Ключ шифрования длиной 1024 бита оказывает меньшую нагрузку на процессор, но считается устаревшим и по техническим характеристикам может не обеспечивать надежное шифрование. Также есть вероятность, что имеющееся оборудование несовместимо с SSL-сертификатами с длиной ключа 1024 бита.

  Ключ шифрования длиной 2048 бит отвечает современным стандартам шифрования. Однако использование 2048-битного ключа шифрования может привести к дополнительной нагрузке на процессор.

  По умолчанию выбран вариант **2048 бит (большая безопасность)**.

Также можно изменить параметры подключения к Серверу администрирования позже:

- Вы можете изменить порт и номера SSL-портов в разделе **Порты подключения** в свойствах Сервера администрирования. Дополнительную информацию о портах для подключения к Серверу администрирования см. в разделе Порты, используемые Kaspersky Security Center.

- Вы можете изменить длину ключа шифрования при замене сертификата Сервера администрирования утилитой klsetsrvcert с помощью параметра `-o RsaKeyLen:<длина ключа>`.

Шаг 13. Задание адреса Сервера администрирования

Укажите адрес Сервера администрирования одним из следующих способов:

- **Имя DNS-домена**. Этот способ используется в том случае, когда в сети присутствует DNS-сервер, и клиентские устройства могут получить с его помощью адрес Сервера администрирования.
- **NetBIOS-имя**. Этот способ используется, если клиентские устройства получают адрес Сервера администрирования с помощью протокола NetBIOS, или в сети присутствует WINS-сервер.
- **IP-адрес**. Этот способ используется, если Сервер администрирования имеет статический IP-адрес, который в дальнейшем не будет изменяться.

Если вы устанавливаете Kaspersky Security Center на активный узел отказоустойчивого кластера Kaspersky Security Center и создали виртуальный сетевой адаптер, во время подготовки узлов кластера укажите IP-адрес этого адаптера. В противном случае введите IP-адрес стороннего балансировщика нагрузки, который вы используете.

Шаг 14. Адрес Сервера для подключения мобильных устройств

Этот шаг мастера установки доступен, если вы выбрали для установки компонент Управление мобильными устройствами.

В окне **Адрес для подключения мобильных устройств** укажите внешний адрес Сервера администрирования для подключения мобильных устройств, которые находятся за пределами локальной сети. Вы можете указать IP-адрес или DNS (Domain Name System) Сервера администрирования.

Шаг 15. Выбор плагинов управления приложениями

Выберите плагины управления приложениями "Лаборатории Касперского", которые требуется установить совместно с Kaspersky Security Center.

Для удобства поиска плагины разделены на группы в зависимости от типа защищаемых объектов.

Шаг 16. Распаковка и установка файлов на жесткий диск

По окончании настройки параметров установки компонентов Kaspersky Security Center вы можете запустить установку файлов на жесткий диск.

Если для запуска установки требуются дополнительные приложения, мастер установки сообщит об этом перед началом установки Kaspersky Security Center в окне **Установка обязательных компонентов**. Необходимые приложения будут установлены автоматически после нажатия на кнопку **Далее**.

На последней странице можно выбрать, какую консоль требуется запустить для работы с Kaspersky Security Center:

- **Запустить Консоль на основе MMC**
- **Запустить как Kaspersky Security Center Web Console**

  Этот параметр доступен, только если на одном из предыдущих шагов вы выбрали установку Kaspersky Security Center Web Console.

Вы можете завершить работу мастера без запуска Kaspersky Security Center. Для этого нажмите на кнопку **Завершить**. Работу с Kaspersky Security Center можно начать позже в любое время.

При первом запуске Консоли администрирования или Kaspersky Security Center Web Console вы можете выполнить первоначальную настройку приложения.

Развертывание отказоустойчивого кластера Kaspersky Security Center

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

Сценарий: развертывание отказоустойчивого кластера Kaspersky Security Center

Отказоустойчивый кластер Kaspersky Security Center обеспечивает высокую доступность Kaspersky Security Center и минимизирует простои Сервера администрирования в случае сбоя. Отказоустойчивый кластер основан на двух идентичных экземплярах Kaspersky Security Center, установленных на двух компьютерах. Один из экземпляров работает как активный узел, а другой – как пассивный. Активный узел управляет защитой клиентских устройств, в то время как пассивный готов взять на себя все функции активного узла в случае отказа активного узла. Когда происходит сбой, пассивный узел становится активным, а активный узел становится пассивным.

Предварительные требования

У вас есть оборудование, соответствующее требованиям для отказоустойчивого кластера.

Этапы

Развертывание приложений "Лаборатории Касперского" состоит из следующих этапов:

1. **Создание учетной записи для служб Kaspersky Security Center**

   Создайте доменную группу (в этом сценарии для группы используется имя "KLAdmins"), и предоставьте права локального администратора группе на обоих узлах и на файловом сервере. Затем создайте две учетные записи пользователей домена (в этом сценарии для этих учетных записей используются имена "ksc" и "rightless"), и добавьте учетные записи в доменную группу KLAdmins.

   Добавьте учетную запись пользователя, под которой будет установлен Kaspersky Security Center, в ранее созданную доменную группу KLAdmins.

2. **Подготовка файлового сервера**

   Подготовьте файловый сервер к работе в составе отказоустойчивого кластера Kaspersky Security Center. Убедитесь, что файловый сервер соответствует аппаратным и программным требованиям, создайте две общие папки для данных Kaspersky Security Center и настройте права доступа к общим папкам.

   Инструкции: Подготовка файлового сервера для отказоустойчивого кластера Kaspersky Security Center.

3. **Подготовка активного и пассивного узлов**

   Подготовьте два устройства с одинаковым аппаратным и программным обеспечением для работы в качестве активного и пассивного узлов.

   Инструкции: Подготовка узлов для отказоустойчивого кластера Kaspersky Security Center.

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

   Выберите любую из поддерживаемых СУБД и установите СУБД на выделенное устройство. Сведения о том, как установить СУБД, см. в документации к ней.

5. **Установка Kaspersky Security Center**

   Установите Kaspersky Security Center в режиме отказоустойчивого кластера на оба узла. Сначала необходимо установить Kaspersky Security Center на устройство, которое вы хотите использовать в качестве активного узла, а затем установить его на пассивный узел.

   Вам нужно установить Kaspersky Security Center Web Console на отдельном устройстве, не являющемся узлом кластера.

   Инструкции: Установка Kaspersky Security Center на узлы отказоустойчивого кластера Kaspersky Security Center.

6. **Тестирование отказоустойчивого кластера**

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

Результаты

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

Об отказоустойчивом кластере Kaspersky Security Center

Отказоустойчивый кластер Kaspersky Security Center обеспечивает высокую доступность Kaspersky Security Center и минимизирует простои Сервера администрирования в случае сбоя. Отказоустойчивый кластер основан на двух идентичных экземплярах Kaspersky Security Center, установленных на двух компьютерах. Один из экземпляров работает как активный узел, а другой – как пассивный. Активный узел управляет защитой клиентских устройств, в то время как пассивный готов взять на себя все функции активного узла в случае отказа активного узла. Когда происходит сбой, пассивный узел становится активным, а активный узел становится пассивным.

Использование отказоустойчивого кластера не влияет на расчеты, основанные на Руководстве по масштабированию.

Используйте функцию Kaspersky Event Log для устранения неполадок.

Геораспределенный отказоустойчивый кластер не поддерживается Kaspersky Security Center. Развертывание отказоустойчивого кластера Kaspersky Security Center возможно только в пределах одной географической площадки.

Условия переключения

Отказоустойчивый кластер переключает управление защитой клиентских устройств с активного узла на пассивный, если на активном узле происходит любое из следующих событий:

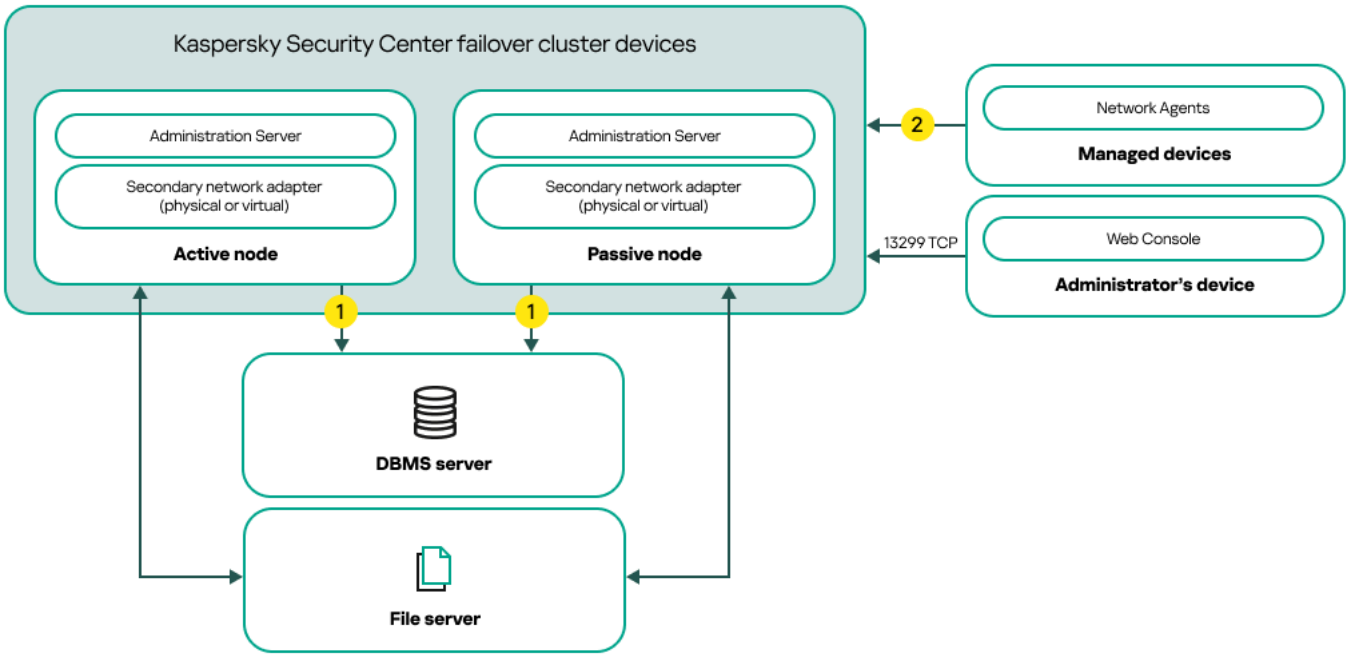
- Активный узел сломан из-за программного или аппаратного сбоя.
- Активный узел был временно остановлен для проведения технических работ.
- По крайней мере, одна из служб (или процессов) Kaspersky Security Center завершилась с ошибкой или была намеренно остановлена пользователем. К службам Kaspersky Security Center относятся: kladminserver, klnagent, klactprx и klwebsrv.
- Сетевое соединение между активным узлом и хранилищем на файловом сервере было прервано или разорвано.

Отказоустойчивый кластер Kaspersky Security Center управляет всеми службами Kaspersky Security Center автоматически. Не перезапускайте службы вручную.

Схемы развертывания

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

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

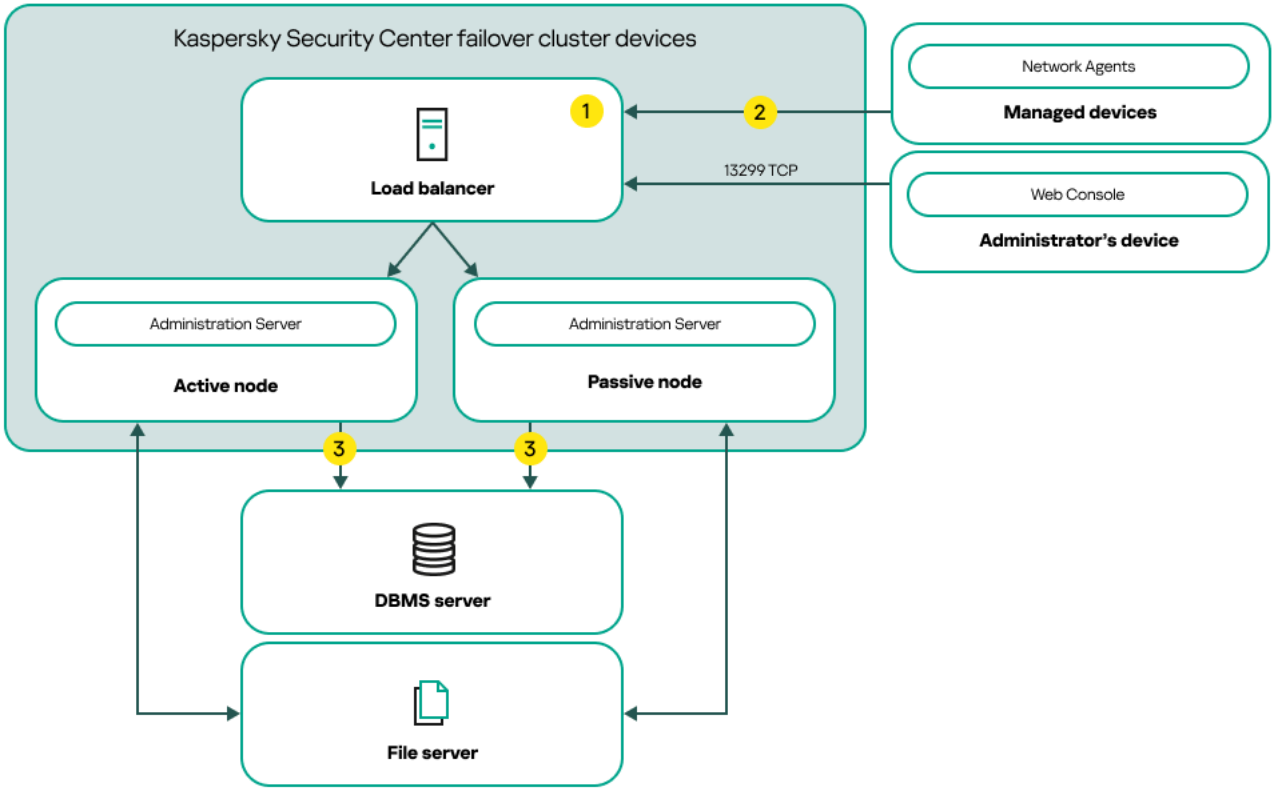


Схема, в которой используется дополнительный сетевой адаптер

Условные обозначения схемы:

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

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



Схема, в которой используется сторонняя балансировка нагрузки

Условные обозначения схемы:

1 На устройстве балансировщика нагрузки откройте все порты Сервера администрирования: TCP 13000, UDP 13000, TCP 13299 и TCP 17000.

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

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

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

Подготовка файлового сервера для отказоустойчивого кластера Kaspersky Security Center

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

Чтобы подготовить файловый сервер:

1. Убедитесь, что файловый сервер соответствует аппаратным и программным требованиям.
2. Убедитесь, что либо файловый сервер и оба узла (активный и пассивный) включены в один домен, либо файловый сервер является контроллером домена.

3. На файловом сервере создайте две общие папки. Один из них используется для хранения информации о состоянии отказоустойчивого кластера. Другая используется для хранения данных и параметров Kaspersky Security Center. Вам нужно будет указать пути к общим папкам при установке Kaspersky Security Center.

4. Предоставьте права полного доступа (как права общего доступа, так и NTFS-разрешения) к созданным общим папкам для следующих учетных записей пользователей и групп:

   - Доменная группа KLAdmins.
   - Учетные записи пользователей $<node1> и $<node2>. Здесь <node1> и <node2> – это имена устройств активного и пассивного узлов.

Файловый сервер подготовлен. Чтобы развернуть отказоустойчивый кластер Kaspersky Security Center, следуйте инструкциям этого сценария.

Подготовка узлов для отказоустойчивого кластера Kaspersky Security Center

Подготовьте два устройства к работе в качестве активного и пассивного узлов для отказоустойчивого кластера Kaspersky Security Center.

Чтобы подготовить узлы для отказоустойчивого кластера Kaspersky Security Center:

1. Убедитесь, что у вас есть два устройства, соответствующих аппаратным и программным требованиям. Эти устройства будут действовать как активный и пассивный узлы отказоустойчивого кластера.

2. Убедитесь, что файловый сервер и оба узла включены в один домен.

3. Выполните одно из следующих действий:

   - На каждом из узлов настройте дополнительный сетевой адаптер.

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

     Убедитесь, что выполняются следующие условия:

     - Дополнительные сетевые адаптеры выключены.

       Вы можете создать дополнительные сетевые адаптеры в отключенном состоянии или отключить их после создания.

     - Дополнительные сетевые адаптеры на обоих узлах должны иметь одинаковый IP-адрес.

   - Используйте сторонний балансировщик нагрузки. Например, вы можете использовать сервер nginx. В этом случае сделайте следующее:

     a. Выделите отдельное устройство с операционной системой Linux с установленным nginx.

     b. Настройте балансировку нагрузки. Установите активный узел в качестве основного сервера и пассивный узел в качестве резервного сервера.

c. На сервере nginx откройте все порты Сервера администрирования: TCP 13000, UDP 13000, TCP 13299 и TCP 17000.

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

4. Перезагрузите оба узла и файловый сервер.

5. Сопоставьте две общие папки, которые вы создали во время этапа подготовки файлового сервера, к каждому из узлов. Вам нужно сопоставить общие папки как сетевые диски. При сопоставлении папок вы можете выбрать любые свободные буквы дисков. Для доступа к общим папкам используйте учетные данные учетной записи пользователя, которую вы создали на шаге 1 сценария.

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

Установка Kaspersky Security Center на узлы отказоустойчивого кластера Kaspersky Security Center

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

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

Чтобы установить Kaspersky Security Center на активный узел отказоустойчивого кластера Kaspersky Security Center:

1. Запустите исполняемый файл ksc_15.1_<build number>_full_<language>.exe.

   Откроется окно с выбором приложений "Лаборатории Касперского" для установки. В окне с выбором приложений по ссылке **Установка Сервера администрирования Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

2. Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

   - **Положения и условия настоящего Лицензионного соглашения**
   - **Политику конфиденциальности, которая описывает обработку данных**

   Установка приложения будет продолжена после установки обоих флажков.

   Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку приложения, нажав на кнопку **Отмена**.

3. Выберите **Первичный узел отказоустойчивого кластера Kaspersky Security Center**, чтобы установить приложение на активный узел.

4. В окне **Общая папка** выполните следующее:

   - В полях **Общая папка состояний** и **Общая папка данных** укажите пути к общим папкам, которые вы создали на файловом сервере во время его подготовки.
   - В полях **Общая папка состояний диска** и **Общая папка данных диска** выберите сетевые диски, к которым вы подключили общие папки во время подготовки узлов.
   - Выберите режим подключения кластера: через дополнительный сетевой адаптер или сторонний балансировщик нагрузки.

5. Выполните другие шаги выборочной установки, начиная с шага 3.

   На шаге 13 укажите IP-адрес дополнительного сетевого адаптера, если вы создали адаптер во время подготовки узлов кластера. В противном случае введите IP-адрес стороннего балансировщика нагрузки, который вы используете.

Приложение Kaspersky Security Center установлено на активном узле.

Чтобы установить Kaspersky Security Center на пассивный узел отказоустойчивого кластера Kaspersky Security Center:

1. Запустите исполняемый файл ksc_15.1_<build number>_full_<language>.exe.

   Откроется окно с выбором приложений "Лаборатории Касперского" для установки. В окне с выбором приложений по ссылке **Установка Сервера администрирования Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

2. Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

   - **Положения и условия настоящего Лицензионного соглашения**
   - **Политику конфиденциальности, которая описывает обработку данных**

   Установка приложения будет продолжена после установки обоих флажков.

   Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку приложения, нажав на кнопку **Отмена**.

3. Выберите **Вторичный узел отказоустойчивого кластера Kaspersky Security Center**, чтобы установить приложение на пассивный узел.

4. В окне **Общая папка** в поле **Общая папка состояний** укажите путь к общей папке с информацией о состоянии кластера, который вы создали на файловом сервере во время его подготовки.

5. Нажмите на кнопку **Установить**. После завершения установки нажмите на кнопку **Готово**.

Приложение Kaspersky Security Center установлено на пассивный узел. Теперь вы можете протестировать отказоустойчивый кластер Kaspersky Security Center, чтобы убедиться, что вы корректно его настроили и кластер работает правильно.

Запуск и остановка узлов кластера вручную

Вам может потребоваться остановить весь отказоустойчивый кластер Kaspersky Security Center или временно отключить один из узлов кластера для обслуживания. В этом случае следуйте инструкциям этого раздела. Не пытайтесь запускать или останавливать службы или процессы, связанные с отказоустойчивым кластером, с помощью других средств. Это может привести к потере данных.

Запуск и остановка всего отказоустойчивого кластера для обслуживания

Чтобы запустить или остановить весь отказоустойчивый кластер:

1. На активном узле перейдите в папку <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
2. Откройте командную строку и выполните одну из следующих команд:
   - Чтобы остановить кластер, выполните: `klfoc -stopcluster --stp klfoc`
   - Чтобы запустить кластер, на обоих узлах кластера выполните: `klfoc -startcluster --stp klfoc`

Отказоустойчивый кластер запускается или останавливается в зависимости от команды.

Обслуживание одного из узлов

Для обслуживания одного из узлов:

1. На активном узле остановите отказоустойчивый кластер с помощью команды `klfoc -stopcluster --stp klfoc`.
2. На узле, который вы хотите обслуживать, перейдите в папку <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
3. Откройте командную строку и отключите узел от кластера, выполнив команду `detach_node.cmd`.
4. На активном узле запустите отказоустойчивый кластер с помощью команды `klfoc -startcluster --stp klfoc`.
5. Выполните работы по техническому обслуживанию.
6. На активном узле остановите отказоустойчивый кластер с помощью команды `klfoc -stopcluster --stp klfoc`.
7. На обслуживаемом узле перейдите в папку <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

8. Откройте командную строку и подключите узел к кластеру, выполнив команду `attach_node.cmd`.

9. На активном узле запустите отказоустойчивый кластер с помощью команды `klfoc -startcluster --stp klfoc`.

Узел обслуживается и подключается к отказоустойчивому кластеру.

Установка Сервера администрирования на отказоустойчивом кластере Windows Server

Процедура установки Сервера администрирования на отказоустойчивом кластере отличается как от стандартной, так и от выборочной установки на автономном устройстве.

> Георазпределенный отказоустойчивый кластер не поддерживается для Windows. Развертывание отказоустойчивого кластера Windows Server возможно только в пределах одной географической площадки, обеспечивающей высокую доступность сети и быстрое время ответа между узлами кластера.

Выполните процедуру, описанную в этом разделе, на узле, который содержит общее хранилище данных кластера.

Чтобы установить Сервер администрирования Kaspersky Security Center на кластер,

запустите исполняемый файл ksc_<номер версии>.<номер сборки>_full_<язык локализации>.exe.

Откроется окно с выбором приложений "Лаборатории Касперского" для установки. В окне с выбором приложений по ссылке **Установить Сервер администрирования Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге мастера установки требуется ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и Политикой конфиденциальности.

Вам также может быть предложено ознакомиться с Лицензионными соглашениями и Политиками конфиденциальности на доступные в дистрибутиве Kaspersky Security Center плагины для управления приложениями.

Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми условиями Лицензионного соглашения и Политики конфиденциальности, подтвердите это, установив соответствующие флажки.

Установка приложения будет продолжена после установки обоих флажков.

Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку приложения, нажав на кнопку **Отмена**.

Шаг 2. Выбор типа установки на кластер

Выберите тип установки на кластере:

- **Кластер (установить на всех узлах кластера)**

  Рекомендуется выбрать этот параметр. Если вы выберете этот параметр, Сервер администрирования будет установлен на всех узлах кластера одновременно.

  > На шаге выбора Консоли администрирования для установки требуется выбрать Консоль, которая будет установлена на текущем узле кластера. Если вы устанавливаете Консоль только на узле кластера, в случае сбоя узла вы потеряете доступ к Серверу администрирования. Рекомендуется на этом шаге выбрать Консоль администрирования на основе консоли Microsoft Management Console (MMC) для установки на все узлы кластера. После установки Сервера администрирования установите Kaspersky Security Center Web Console на отдельном устройстве, не являющемся узлом кластера. Это позволяет управлять Сервером администрирования с помощью Kaspersky Security Center Web Console в случае сбоя узла кластера.

- **Локально (установить только на это устройство)**

  Если вы выберете этот параметр, Сервер администрирования будет установлен только на текущем узле, как на автономном сервере, и Сервер администрирования не будет работать как кластерное приложение. Например, вы можете выбрать этот параметр для экономии свободного пространства в общем хранилище, если отказоустойчивость не требуется для Сервера администрирования. В случае выхода из строя текущего узла вам придется установить Сервер администрирования на другой узел и восстановить состояние Сервера администрирования из резервной копии данных.

Дальнейшие действия такие же, как при использовании стандартного или выборочного способа установки, начиная с шага выбора способа установки.

Шаг 3. Указание имени виртуального Сервера администрирования

Укажите сетевое имя нового виртуального Сервера администрирования. Вы сможете использовать это имя для подключения Консоли администрирования или Kaspersky Security Center Web Console к Серверу администрирования.

Указанное имя должно отличаться от имени кластера.

Шаг 4. Указание параметров сети виртуального Сервера администрирования

Чтобы указать сетевые данные нового экземпляра виртуального Сервера администрирования:

1. В разделе **Сеть для использования** выберите сеть домена, к которой подключен текущий узел кластера.
2. Выполните одно из следующих действий:
   - Если DHCP используется в выбранной сети для назначения IP-адресов, выберите параметр **Использовать DHCP**.
   - Если DHCP не используется в выбранной сети, укажите требуемый IP-адрес.

     Указанный вами IP-адрес должен отличаться от IP-адреса кластера.
3. Нажмите на кнопку **Добавить**, чтобы применить указанные параметры.

Вы сможете использовать автоматически назначенный или указанный IP-адрес для подключения Консоли администрирования или Kaspersky Security Center Web Console к Серверу администрирования.

Шаг 5. Указание группы кластеров

Группа кластера – это особая роль отказоустойчивого кластера, которая содержит общие ресурсы для всех узлов. У вас есть два варианта:

- Создание новой кластерной группы.

  Этот вариант рекомендуется в большинстве случаев. Новая группа кластера будет содержать все общие ресурсы, относящиеся к экземпляру Сервера администрирования.

- Выбор существующей группы кластеров.

  Выберите этот параметр, если вы хотите использовать общий ресурс, который уже связан с существующей группой кластера. Например, вы можете использовать этот вариант, если хотите использовать хранилище, связанное с существующей группой кластера, и если нет другого доступного хранилища для новой группы кластера.

Шаг 6. Выбор кластерного хранилища данных

Чтобы выбрать кластерное хранилище данных:

1. В разделе **Доступные хранилища** выберите хранилище, в которое будут установлены общие ресурсы экземпляра виртуального Сервера администрирования.
2. Если выбранное хранилище данных содержит несколько томов, в разделе **Доступные разделы на диске** выберите нужный том.
3. В поле **Путь установки** введите путь к общему хранилищу данных, в который будут установлены ресурсы экземпляра виртуального Сервера администрирования.

Хранилище данных выбрано.

Шаг 7. Указание учетной записи для удаленной установки

Укажите имя пользователя и пароль, которые будут использоваться для удаленной установки экземпляра виртуального Сервера администрирования на пассивный узел кластера.

Для указанной вами учетной записи должны быть предоставлены права администратора на всех узлах кластера.

Шаг 8. Выбор компонентов для установки

Выберите компоненты Сервера администрирования Kaspersky Security Center, которые вы хотите установить:

- **Управление мобильными устройствами**. Установите этот флажок, если требуется создать инсталляционные пакеты для мобильных устройств во время работы мастера установки Kaspersky Security Center. Вы можете также создать инсталляционные пакеты для мобильных устройств вручную, после установки Сервера администрирования средствами Консоли администрирования.
- **Агент SNMP**. Получает статистическую информацию для Сервера администрирования по протоколу SNMP. Компонент доступен при установке приложения на устройство с установленным компонентом SNMP.

  После установки Kaspersky Security Center необходимые для получения статистической информации mib-файлы будут расположены в папке установки приложения во вложенной папке SNMP.

Компоненты Агент администрирования и Консоль администрирования не отображаются в списке компонентов. Эти компоненты устанавливаются автоматически, их установку отменить невозможно.

На этом шаге мастера также следует указать папку для установки компонентов Сервера администрирования. По умолчанию компоненты устанавливаются в папку <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Если папки с таким названием нет, она будет создана автоматически в процессе установки. Вы можете изменить папку назначения с помощью кнопки **Обзор**.

Шаг 9. Выбор размера сети

Укажите размер сети, в которой устанавливается Kaspersky Security Center. В зависимости от количества устройств в сети мастер настраивает параметры установки и отображение интерфейса приложения.

В таблице ниже перечислены параметры установки приложения и отображения интерфейса при выборе разных размеров сети.

Зависимость параметров установки от выбора размеров сети

Параметры	1–100 управляемых устройств	101–1000 управляемых устройств	1001–5000 управляемых устройств	Более 5000 управляемых устройств
Отображение в дереве консоли узла подчиненных и виртуальных Серверов администрирования и всех параметров, связанных с подчиненными и виртуальными Серверами (только в Консоли администрирования на базе MMC)	Отсутствует	Отсутствует	Присутствует	Присутствует
Отображение с разделами **Безопасность** в окнах свойств Сервера администрирования и групп администрирования (доступно только в Консоли администрирования на базе MMC)	Отсутствует	Отсутствует	Присутствует	Присутствует
Распределение времени запуска задачи обновления на клиентских устройствах случайным образом	Отсутствует	в интервале 5 минут	в интервале 10 минут	в интервале 10 минут

При подключении Сервера администрирования к серверу базы данных MySQL 5.7 или SQL Express не рекомендуется использовать приложение для управления более чем 10 000 устройств. Для системы управления базами данных MariaDB максимальное рекомендуемое количество управляемых устройств составляет 20 000.

Шаг 10. Выбор базы данных

На этом шаге мастера выберите одну из следующих систем управления базами данных (СУБД), которая будет использоваться для хранения базы данных Сервера администрирования:

- **Microsoft SQL Server или SQL Server Express**
- **MySQL или MariaDB**
- **PostgreSQL или Postgres Pro**

Рекомендуется устанавливать Сервер администрирования на выделенный сервер, а не на контроллер домена. Если вы устанавливаете Kaspersky Security Center на сервер, выполняющий роль контроллера домена только для чтения (RODC), Microsoft SQL Server (SQL Express) не должен быть установлен локально (на этом же устройстве). В этом случае рекомендуется установить Microsoft SQL Server (SQL Express) удаленно (на другое устройство) или использовать MySQL, MariaDB или PostgreSQL, если вам нужно установить СУБД локально.

Структура базы данных Сервера администрирования представлена в файле klakdb.chm, который находится в папке установки Kaspersky Security Center. Этот файл также доступен в архиве на портале "Лаборатории Касперского": klakdb.zip.

Шаг 11. Настройка параметров SQL-сервера

На этом шаге мастера укажите следующие параметры подключения в зависимости от выбранной вами системы управления базами данных (СУБД):

- Если вы выбрали **Microsoft SQL Server или SQL Server Express** на предыдущем шаге:

  - В поле **Имя экземпляра SQL-сервера** укажите имя SQL-сервера, установленного в сети. При помощи кнопки **Обзор** вы можете открыть список всех SQL-серверов, установленных в сети. По умолчанию поле не заполнено.

    Если вы подключаетесь к SQL Server через пользовательский порт, то вместе с именем экземпляра SQL Server укажите через запятую номер порта, например:

    ```
    SQL_Server_host_name,1433
    ```

    Если вы защищаете соединение между Сервером администрирования и SQL Server с помощью сертификата, укажите в поле **Имя экземпляра SQL-сервера** то же имя экземпляра, которое использовалось при создании сертификата. Если вы используете именованный экземпляр SQL Server, вместе с именем экземпляра SQL Server укажите через запятую номер порта, например:

    ```
    SQL_Server_name,1433
    ```

    Если вы используете несколько экземпляров SQL Server на одном устройстве, дополнительно укажите через обратную косую черту имя экземпляра, например:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    Если для SQL Server в корпоративной сети включена функция Always On, укажите имя прослушивателя группы доступности в поле **Имя экземпляра SQL-сервера**. Обратите внимание, что Сервер администрирования поддерживает только режим доступности с синхронной фиксацией, когда включена функция Always On.

  - В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

  Если на этом шаге вы хотите установить SQL-сервер на то устройство, с которого производите установку Kaspersky Security Center, нужно прервать установку и запустить ее снова после установки SQL-сервера. Поддерживаемые версии SQL Server перечислены в требованиях к системе.

  Если вы хотите установить SQL-сервер на удаленное устройство, прерывать работу мастера установки Kaspersky Security Center не требуется. Установите SQL Server и вернитесь к установке Kaspersky Security Center.

- Если вы выбрали **MySQL или MariaDB** на предыдущем шаге:

  - В поле **Имя экземпляра SQL-сервера** укажите имя экземпляра СУБД. По умолчанию используется IP-адрес устройства, на которое устанавливается Kaspersky Security Center.

  - В поле **Порт** укажите порт для подключения Сервера администрирования к СУБД. По умолчанию установлен порт 3306.

  - В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

- Если вы выбрали **PostgreSQL или Postgres Pro** на предыдущем шаге:

  - В поле **PostgreSQL или Postgres Pro Server** укажите имя экземпляра СУБД. По умолчанию используется IP-адрес устройства, на которое устанавливается Kaspersky Security Center.

  - В поле **Порт** укажите порт для подключения Сервера администрирования к СУБД. По умолчанию установлен порт 5432.

В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

Шаг 12. Выбор режима аутентификации

Определите режим аутентификации, который будет использоваться при подключении Сервера администрирования к системе управления базами данных (СУБД).

В зависимости от выбранной СУБД вы можете выбрать следующие режимы аутентификации:

- Для SQL Express или Microsoft SQL Server выберите один из следующих вариантов:

  - **Режим аутентификации Microsoft Windows**. В этом случае при проверке прав будет использоваться учетная запись для запуска Сервера администрирования.

  - **Режим аутентификации SQL-сервера**. В случае выбора этого варианта для проверки прав будет использоваться указанная в окне учетная запись. Заполните поля **Учетная запись** и **Пароль**.

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

  Приложение проверяет, доступна ли база данных для обоих режимов аутентификации. Если база данных недоступна, отображается сообщение об ошибке и вам нужно указать правильные учетные данные.

  Если база данных Сервера администрирования находится на другом устройстве и учетная запись Сервера администрирования не имеет доступа к серверу базы данных, то при установке или обновлении Сервера администрирования следует использовать режим аутентификации SQL-сервера. Это может происходить в случае, когда устройство с базой данных находится не в домене, или Сервер администрирования установлен под учетной записью LocalSystem.

Для MySQL, MariaDB, PostgreSQL или Postgres Pro укажите учетную запись и пароль.

Шаг 13. Выбор учетной записи для запуска Сервера администрирования

Выберите учетную запись, под которой Сервер администрирования будет запускаться как служба.

- **Создать учетную запись автоматически**. Приложение создает локальную учетную запись KL-AK-*, под которой будет запускаться служба Сервера администрирования kladminserver.

  Вы можете выбрать этот вариант, если вы планируете разместить папку общего доступа и СУБД на том же устройстве, что и Сервер администрирования.

- **Выбрать учетную запись**. Служба Сервера администрирования (kladminserver) будет запускаться под выбранной вами учетной записью.

Вам потребуется выбрать доменную учетную запись, например, если вы планируете использовать в качестве СУБД SQL-сервер любого выпуска, в том числе SQL-express, расположенный на другом устройстве, и/или если вы планируете разместить папку общего доступа на другом устройстве.

Kaspersky Security Center поддерживает управляемые учетные записи службы (MSA) и групповые управляемые учетные записи службы (gMSA). Если такие учетные записи используются в вашем домене, вы можете выбрать одну из них в качестве учетной записи для службы Сервера администрирования.

Прежде чем выбрать MSA или gMSA, необходимо установить учетную запись на том же устройстве, на котором вы хотите установить Сервер администрирования. Если учетная запись еще не установлена, отмените установку Сервера администрирования, установите учетную запись и перезапустите установку Сервера администрирования. Подробнее об установке управляемых учетных записей служб на локальном устройстве см. в официальной документации Microsoft.

Чтобы указать MSA или gMSA:

1. Нажмите на кнопку **Обзор**.
2. В появившемся окне нажмите на кнопку **Object type**.
3. Выберите тип **Учетная запись для служб** и нажмите на кнопку **OK**.
4. Выберите нужную учетную запись и нажмите на кнопку **OK**.

Выбранная вами учетная запись должна обладать различными правами в зависимости от того, какую СУБД вы планируете использовать.

Из соображений безопасности не делайте учетную запись, под которой запускается Сервер администрирования, привилегированной.

Учетную запись Сервера администрирования изменить позже невозможно. Для использования другой учетной записи Сервера администрирования нужно переустановить отказоустойчивый кластер.

Шаг 14. Выбор учетной записи для запуска служб Kaspersky Security Center

Выберите учетную запись, под которой будут запускаться службы Kaspersky Security Center на этом устройстве:

- **Создать учетную запись автоматически**. Kaspersky Security Center создает локальную учетную запись KlScSvc на этом устройстве в группе kladmins. Службы Kaspersky Security Center будут запускаться под созданной учетной записью.
- **Выбрать учетную запись**. Службы Kaspersky Security Center будут запускаться под выбранной вами учетной записью.

  Вам потребуется выбрать доменную учетную запись, например, если вы планируете сохранять отчеты в папке, расположенной на другом устройстве, или же если этого требует политика безопасности в вашей организации. Также вам может потребоваться выбрать доменную учетную запись при установке Сервера администрирования на отказоустойчивый кластер.

Из соображений безопасности не делайте учетную запись, под которой запускаются службы, привилегированной.

Под выбранной учетной записью будут запускаться службы прокси-сервера KSN (ksnproxy), прокси-сервера активации "Лаборатории Касперского" (klactprx) и портала авторизации "Лаборатории Касперского" (klwebsrv).

Шаг 15. Определение папки общего доступа

Определите место размещения и название папки общего доступа, которая будет использоваться для следующих целей:

- хранения файлов, необходимых для удаленной установки приложений (файлы копируются на Сервер администрирования при создании инсталляционных пакетов);
- размещения обновлений, копируемых с источника обновлений на Сервер администрирования.

К этому ресурсу будет открыт общий доступ на чтение для всех пользователей.

Вы можете выбрать один из двух вариантов:

- **Создать папку общего доступа**. Создание новой папки. Укажите путь к папке в расположенном ниже поле.
- **Выбрать существующую папку общего доступа**. Выбор папки общего доступа из числа уже существующих.

Папка общего доступа может размещаться как локально на устройстве, с которого производится установка, так и удаленно, на любом из клиентских устройств, входящих в состав сети организации. Вы можете указать папку общего доступа с помощью кнопки **Обзор** или вручную, введя в соответствующем поле UNC-путь (например, \\server\Share).

По умолчанию создается локальная папка KLSHARE в папке, заданной для установки компонентов Kaspersky Security Center.

Вы можете определить общую папку позже, если нужно.

Шаг 16. Настройка параметров подключения к Серверу администрирования

Настройте параметры подключения к Серверу администрирования:

- **Порт**

  Номер порта, по которому выполняется подключение к Серверу администрирования.

  По умолчанию установлен порт 14000.

- **SSL-порт**

  Номер SSL-порта, по которому осуществляется защищенное подключение к Серверу администрирования с использованием протокола SSL.

  По умолчанию установлен порт 13000.

- **Длина ключа шифрования**

  Выберите длину ключа шифрования: 1024 бита или 2048 бит.

  Ключ шифрования длиной 1024 бита оказывает меньшую нагрузку на процессор, но считается устаревшим и по техническим характеристикам может не обеспечивать надежное шифрование. Также есть вероятность, что имеющееся оборудование несовместимо с SSL-сертификатами с длиной ключа 1024 бита.

  Ключ шифрования длиной 2048 бит отвечает современным стандартам шифрования. Однако использование 2048-битного ключа шифрования может привести к дополнительной нагрузке на процессор.

  По умолчанию выбран вариант **2048 бит (большая безопасность)**.

Также можно изменить параметры подключения к Серверу администрирования позже:

- Вы можете изменить порт и номера SSL-портов в разделе **Порты подключения** в свойствах Сервера администрирования. Дополнительную информацию о портах для подключения к Серверу администрирования см. в разделе Порты, используемые Kaspersky Security Center.

- Вы можете изменить длину ключа шифрования при замене сертификата Сервера администрирования утилитой klsetsrvcert с помощью параметра `-o RsaKeyLen:<длина ключа>`.

Шаг 17. Задание адреса Сервера администрирования

Задайте адрес Сервера администрирования. Вы можете выбрать один из следующих вариантов:

- **Имя DNS-домена**. Этот способ используется в том случае, когда в сети присутствует DNS-сервер, и клиентские устройства могут получить с его помощью адрес Сервера администрирования.

- **NetBIOS-имя**. Этот способ используется, если клиентские устройства получают адрес Сервера администрирования с помощью протокола NetBIOS, или в сети присутствует WINS-сервер.

- **IP-адрес**. Этот способ используется, если Сервер администрирования имеет статический IP-адрес, который в дальнейшем не будет изменяться.

Шаг 18. Адрес Сервера для подключения мобильных устройств

Этот шаг мастера установки доступен, если вы выбрали для установки компонент Управление мобильными устройствами.

В окне **Адрес для подключения мобильных устройств** укажите внешний адрес Сервера администрирования для подключения мобильных устройств, которые находятся за пределами локальной сети. Вы можете указать IP-адрес или DNS (Domain Name System) Сервера администрирования.

Шаг 19. Распаковка и установка файлов на жесткий диск

По окончании настройки параметров установки компонентов Kaspersky Security Center вы можете запустить установку файлов на жесткий диск.

Если для запуска установки требуются дополнительные приложения, мастер установки сообщит об этом перед началом установки Kaspersky Security Center в окне **Установка обязательных компонентов**. Необходимые приложения будут установлены автоматически после нажатия на кнопку **Далее**.

На последней странице можно выбрать, какую консоль требуется запустить для работы с Kaspersky Security Center:

- **Запустить Консоль на основе MMC**
- **Запустить как Kaspersky Security Center Web Console**

  Этот параметр доступен, только если на одном из предыдущих шагов вы выбрали установку Kaspersky Security Center Web Console.

Вы можете завершить работу мастера без запуска Kaspersky Security Center. Для этого нажмите на кнопку **Завершить**. Работу с Kaspersky Security Center можно начать позже в любое время.

При первом запуске Консоли администрирования или Kaspersky Security Center Web Console вы можете выполнить первоначальную настройку приложения.

Установка Сервера администрирования в тихом режиме

Сервер администрирования может быть установлен в тихом режиме, то есть без интерактивного ввода параметров установки.

Чтобы установить Сервер администрирования на локальном устройстве в тихом режиме:

1. Прочитайте Лицензионное соглашение. Используйте команду ниже, только если вы поняли и принимаете условия Лицензионного соглашения.
2. Прочитайте Политику конфиденциальности. Используйте команду ниже, только если вы понимаете и соглашаетесь с тем, что мои данные будут обрабатываться и передаваться (в том числе в третьи страны), как описано в Политике конфиденциальности.
3. Выполните команду

```
setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1 <setup_parameters>"
```

где `setup_parameters` – список параметров и их значений, отделенных друг от друга пробелом (`PARAM1=PARAM1VAL PARAM2=PARAM2VAL`). Файл setup.exe расположен в папке Server внутри дистрибутива Kaspersky Security Center.

Имена и возможные значения параметров, которые можно использовать при установке Сервера администрирования в тихом режиме, приведены в таблице ниже.

Имя параметра	Описание параметра	Доступные значения
EULA	Согласие с условиями Лицензионного соглашения.	• 1 – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Лицензионного соглашения. • Другое значение или не задано – не согласны с условиями Лицензионного соглашения (установка не выполняется).
PRIVACYPOLICY	Согласие с условиями Политики конфиденциальности.	• 1 – Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности. Я подтверждаю, что полностью прочитал(а) и понимаю Политику конфиденциальности. • Другое значение или не задано – Я не принимаю условия Политики конфиденциальности (установка не выполняется).
INSTALLATIONMODETYPE	Тип установки Сервера администрирования.	• Standard – стандартная установка. • Custom – выборочная установка.
INSTALLDIR	Путь к папке установки Сервера администрирования.	Строковое значение.
ADDLOCAL	Список компонентов (через запятую) Сервера администрирования для установки.	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Минимальный достаточный для корректной установки Сервера администрирования список компонентов: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`.
NETRANGETYPE	Размер сети (количество устройств в сети).	• NRT_1_100 – от 1 до 100 устройств. • NRT_100_1000 – от 101 до 1000 устройств. • NRT_GREATER_1000 – более 1000 устройств.
SRV_ACCOUNT_TYPE	Способ задания учетной записи, под которой Сервер администрирования будет запускаться как служба.	• SrvAccountDefault – учетная запись создается автоматически. • SrvAccountUser – учетная запись пользователя задана вручную. В этом случае требуется задать значения параметров `SERVERACCOUNTNAME` и `SERVERACCOUNTPWD`.
SERVERACCOUNTNAME	Имя учетной записи, под которой Сервер администрирования будет запускаться как служба. Требуется задать значение параметра, если SRV_ACCOUNT_TYPE=SrvAccountUser.	Строковое значение.

Имя параметра	Описание параметра	Доступные значения
SERVERACCOUNTPWD	Пароль учетной записи, под которой Сервер администрирования будет запускаться как служба. Требуется задать значение параметра, если SRV_ACCOUNT_TYPE=SrvAccountUser.	Строковое значение.
SERVERCER	Длина ключа для сертификата Сервера администрирования (в битах).	• 1 – длина ключа для сертификата Сервера администрирования составляет 2048 бит. • Значение не задано – длина ключа для сертификата Сервера администрирования составляет 1024 бит.
DBTYPE	Тип базы данных, которая будет использоваться для размещения информационной базы данных Сервера администрирования. Этот параметр является обязательным.	• MySQL – будет использоваться база данных MySQL или MariaDB. В этом случае следует задать значения параметров `MYSQLSERVERNAME`, `MYSQLSERVERPORT`, `MYSQLDBNAME`, `MYSQLACCOUNTNAME` и `MYSQLACCOUNTPWD`. • MSSQL – будет использоваться база данных Microsoft SQL Server (SQL Express). В этом случае следует задать значения параметров `MSSQLSERVERNAME`, `MSSQLDBNAME`, `MSSQLAUTHTYPE`. • POSTGRES – будет использоваться база данных PostgreSQL или Postgres Pro. В этом случае следует задать значения параметров `POSTGRESSERVERNAME`, `POSTGRESSERVERPORT`, `POSTGRESDBNAME`, `POSTGRESACCOUNTNAME` и `POSTGRESACCOUNTPWD`.
MYSQLSERVERNAME	Полное имя SQL Server. Требуется задать значение параметра, если DBTYPE=MySQL.	Строковое значение.
MYSQLSERVERPORT	Номер порта для подключения к SQL-серверу. Требуется задать значение параметра, если DBTYPE=MySQL.	Числовое значение.
MYSQLDBNAME	Имя базы данных, которая будет создана для размещения данных Сервера администрирования. Требуется задать значение параметра, если DBTYPE=MySQL.	Строковое значение.
MYSQLACCOUNTNAME	Имя учетной записи для подключения к базе. Требуется задать значение параметра, если DBTYPE=MySQL.	Строковое значение.
MYSQLACCOUNTPWD	Пароль учетной записи для подключения к базе. Требуется задать значение параметра, если DBTYPE=MySQL.	Строковое значение.
MSSQLSERVERNAME	Полное имя SQL Server. Требуется задать значение параметра, если DBTYPE=MSSQL.	Строковое значение.
MSSQLDBNAME	Имя базы данных. Требуется задать значение параметра, если DBTYPE=MSSQL.	Строковое значение.
MSSQLAUTHTYPE	Тип авторизации при подключении к SQL-серверу. Требуется задать значение параметра, если DBTYPE=MSSQL.	• Windows – режим аутентификации Microsoft Windows. • SQLServer – режим аутентификации SQL-сервера. В этом случае требуется задать значения параметров `MSSQLACCOUNTNAME` и `MSSQLACCOUNTPWD`.
MSSQLACCOUNTNAME	Имя учетной записи для подключения к SQL-серверу. Требуется задать значение параметра, если MSSQLAUTHTYPE=SQLServer.	Строковое значение.
MSSQLACCOUNTPWD	Пароль учетной записи для подключения к SQL-серверу. Требуется задать значение параметра, если MSSQLAUTHTYPE=SQLServer.	Строковое значение.
CREATE_SHARE_TYPE	Способ задания папки общего доступа.	• Create – создать новую папку общего доступа. В этом случае требуется задать значения параметров `SHARELOCALPATH` и `SHAREFOLDERNAME`. • ChooseExisting – выбрать существующую папку. В этом случае требуется задать значение параметра `EXISTSHAREFOLDERNAME`.

Имя параметра	Описание параметра	Доступные значения
SHARELOCALPATH	Путь к локальной папке. Требуется задать значение параметра, если CREATE_SHARE_TYPE=Create	Строковое значение.
SHAREFOLDERNAME	Сетевое имя папки общего доступа. Требуется задать значение параметра, если CREATE_SHARE_TYPE=Create.	Строковое значение.
EXISTSHAREFOLDERNAME	Полный путь к существующей папке общего доступа. Требуется задать значение параметра, если CREATE_SHARE_TYPE=ChooseExisting.	Строковое значение.
SERVERPORT	Номер порта для подключения к Серверу администрирования.	Числовое значение.
SERVERSSLPORT	Номер порта для защищенного подключения к Серверу администрирования с использованием протокола SSL	Числовое значение.
SERVERADDRESS	Адрес Сервера администрирования.	Строковое значение.
MOBILESERVERADDRESS	Адрес Сервера для подключения мобильных устройств.	Строковое значение.

Подробно параметры установки Сервера администрирования описаны в разделе Выборочная установка.

Установка Консоли администрирования на рабочее место администратора

Вы можете установить Консоль администрирования отдельно на рабочее место администратора и управлять Сервером администрирования по сети с помощью этой Консоли.

Чтобы установить Консоль администрирования на рабочее место администратора:

1. Запустите исполняемый файл setup.exe.

   Откроется окно с выбором приложений "Лаборатории Касперского" для установки.

2. В окне с выбором приложений по ссылке **Установить только Консоль администрирования Kaspersky Security Center** запустите мастер установки Консоли администрирования. Следуйте далее указаниям мастера.

3. Выберите папку назначения. По умолчанию это <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console. Если такой папки нет, она будет создана автоматически в процессе установки. Вы можете изменить папку назначения с помощью кнопки **Обзор**.

4. В завершающем окне мастера установки нажмите на кнопку **Запустить**, чтобы начать процесс установки Консоли администрирования.

   По окончании работы мастера Консоль администрирования будет установлена на рабочем месте администратора.

Чтобы установить Консоль администрирования на рабочее место администратора в тихом режиме:

1. Прочитайте Лицензионное соглашение. Используйте команду ниже, только если вы поняли и принимаете условия Лицензионного соглашения.

2. В папке `Distrib\Console` дистрибутива Kaspersky Security Center запустите файл setup.exe с помощью следующей команды:

   ```
   setup.exe /s /v"EULA=1"
   ```

   Если вы хотите установить все плагины управления из папки `Distrib\Console\Plugins` вместе с Консолью администрирования, выполните следующую команду:

   ```
   setup.exe /s /v"EULA=1" /pALL
   ```

   Если вы хотите указать, какие плагины управления устанавливать из папки `Distrib\Console\Plugins` вместе с Консолью администрирования, укажите плагины управления после ключа "/p" и разделите их точкой с запятой:

   ```
   setup.exe /s /v"EULA=1" /pP1;P2;P3
   ```

   Здесь `P1`, `P2`, `P3` – имена плагинов управления, которые соответствуют именам папок плагинов управления в папке `Distrib\Console\Plugins`. Например:

   ```
   setup.exe /s /v"EULA=1" /pKES4Mac;KESS;MDM4IOS
   ```

Консоль администрирования и плагины управления (если они были указаны) будут установлены на рабочее место администратора.

После установки Консоли администрирования следует подключиться к Серверу администрирования. Для этого нужно запустить Консоль администрирования и в открывшемся окне указать имя устройства или IP-адрес устройства, на котором установлен Сервер администрирования, а также параметры учетной записи для подключения к нему. После установления соединения с Сервером администрирования можно управлять системой антивирусной защиты с помощью этой Консоли администрирования.

Вы можете удалить Консоль администрирования стандартными средствами установки и удаления приложений Microsoft Windows.

Изменения в системе после установки Kaspersky Security Center

Значок Консоли администрирования

В результате установки Консоли администрирования на вашем устройстве появится значок для запуска Консоли администрирования. Вы можете найти Консоль администрирования в меню **Пуск** → **Приложения** → **Kaspersky Security Center**.

Службы Сервера администрирования и Агента администрирования

Сервер администрирования и Агент администрирования будут установлены на устройстве в качестве служб со свойствами, указанными в таблице ниже. В таблице также указаны атрибуты других служб, которые выполняются на устройстве после установки Сервера администрирования.

Свойства служб Kaspersky Security Center

Компонент	Имя службы	Отображаемое имя службы	Учетная запись
Сервер администрирования	kladminserver	Сервер администрирования Kaspersky Security Center.	Указанная пользователем или специальная, созданная при установке, непривилегированная учетная запись вида KL-AK-*
Агент администрирования	klnagent	Агент администрирования Kaspersky Security Center.	Локальная система
Веб-сервер для работы Kaspersky Security Center Web Console и организации внутреннего портала организации	klwebsrv	Веб-сервер "Лаборатории Касперского"	Специальная непривилегированная учетная запись KlScSvc
Прокси-сервер активации	klactprx	Прокси-сервер активации "Лаборатории Касперского"	Специальная непривилегированная учетная запись KlScSvc
Прокси-сервер KSN	ksnproxy	Прокси-сервер Kaspersky Security Network	Специальная непривилегированная учетная запись KlScSvc

Если вы установите Kaspersky Security Center на узлах отказоустойчивого кластера Kaspersky Security Center, станет доступна служба klfocsvc_klfoc. Службы klnagent_klfoc and klfocsvc_klfoc запускаются под учетной записью локальной системы. Служба kladminserver_klfoc должна запускаться под учетной записью "ksc"; другие службы — под учетной записью "rightless". Учетные записи "ksc" и "rightless" необходимо добавить в группу KLAdmins с правами локального администратора. Для корректной работы Kaspersky Security Center необходимо использовать для запуска служб только учетные записи "ksc" и "rightless". Не рекомендуется использовать другие учетные записи с такими же правами. В таблице ниже приведены свойства служб, которые применяются на устройстве после установки Сервера администрирования на отказоустойчивом кластере Kaspersky Security Center.

Свойства сервисов Kaspersky Security Center, установленных на отказоустойчивом кластере Kaspersky Security Center

Компонент	Имя службы	Отображаемое имя службы	Учетная запись
Сервер администрирования	kladminserver_klfoc	Сервер администрирования Kaspersky Security Center.	ksc
Агент администрирования;	klnagent_klfoc	Агент администрирования Kaspersky Security Center.	Локальная система
Веб-сервер для работы Kaspersky Security Center Web Console и организации внутреннего портала организации	klwebsrv_klfoc	Веб-сервер "Лаборатории Касперского"	права отсутствуют
Прокси-сервер активации	klactprx_klfoc	Прокси-сервер активации "Лаборатории Касперского"	права отсутствуют
Прокси-сервер KSN	ksnproxy_klfoc	Прокси-сервер Kaspersky Security Network	права отсутствуют
Отказоустойчивый кластер Kaspersky Security Center	klfocsvc_klfoc	Отказоустойчивый кластер Kaspersky Security Center	Локальная система

Службы Kaspersky Security Center Web Console

Если вы установите Kaspersky Security Center Web Console на устройство, то на нем будут выполняться следующие службы (см. таблицу ниже):

Службы Kaspersky Security Center Web Console

Отображаемое имя службы	Учетная запись
Kaspersky Security Center Service Web Console	NT Service/KSCSvcWebConsole
Kaspersky Security Center Web Console	Сетевая служба

Kaspersky Security Center Product Plugins Server	NT Service/KSCWebConsolePlugin
Kaspersky Security Center Web Console Management Service	Локальная система
Kaspersky Security Center Web Console Message Queue	NT Service/KSCWebConsoleMessageQueue

Серверная версия Агента администрирования

Вместе с Сервером администрирования на устройство будет установлена серверная версия Агента администрирования. Она входит в состав Сервера администрирования, устанавливается и удаляется в его составе и может взаимодействовать только с локально установленным Сервером администрирования. Настраивать параметры подключения Агента к Серверу администрирования не требуется: настройка реализована программно с учетом того, что компоненты установлены на одном устройстве. Серверная версия Агента администрирования устанавливается с теми же атрибутами и выполняет те же функции управления приложениями, что и стандартный Агент администрирования. На эту версию будет действовать политика группы администрирования, в которую включено клиентское устройство Сервера администрирования. Для серверной версии Агента администрирования создаются все задачи, предусмотренные для Агента администрирования, за исключением задачи смены Сервера.

Отдельная установка Агента администрирования на устройство с Сервером администрирования невозможна.

Вы можете просматривать свойства служб Сервера и Агента администрирования, а также следить за их работой при помощи стандартных средств администрирования Microsoft Windows: Управление компьютером\Службы. Информация о работе службы Сервера администрирования сохраняется в системном журнале Microsoft Windows на устройстве, где установлен Сервер администрирования, в отдельной ветви журнала событий Kaspersky Event Log.

Не рекомендуется вручную запускать и отключать службы и менять учетные записи в настройках служб. При необходимости вы можете поменять учетную запись службы Сервера администрирования с помощью утилиты klsrvswch. Обратите внимание, что вам нужно запустить утилиту klsrvswch на устройстве Сервера администрирования под учетной записью с правами администратора, которая использовалась для установки Сервера администрирования.

Учетные записи и группы безопасности

По умолчанию инсталлятор Сервера администрирования создает следующие учетные записи:

- KL-AK-*: учетная запись службы Сервера администрирования;
- KlScSvc: учетная запись для прочих служб из состава Сервера администрирования;
- KlPxeUser: учетная запись для развертывания операционных систем.

Если на этапе работы инсталлятора вы выбирали другие учетные записи для службы Сервера администрирования и прочих служб, то будут использованы указанные вами учетные записи.

На устройстве, где установлен Сервер администрирования, также автоматически создаются локальные группы безопасности KLAdmins и KLOperators, с их соответствующими наборами прав.

Не рекомендуется устанавливать Сервер администрирования на контроллере домена. Тем не менее, если вы устанавливаете Сервер администрирования на контроллер домена, то вам нужно запустить приложение установки с правами администратора домена. В этом случае приложение установки автоматически создаст доменные группы безопасности KLAdmins и KLOperators. Если вы устанавливаете Сервер администрирования на устройство, которое не является контроллером домена, то вам нужно запустить приложение установки с правами локального администратора. В этом случае приложение установки автоматически создаст локальные группы безопасности KLAdmins и KLOperators.

При настройке уведомлений по электронной почте вам может потребоваться завести учетную запись на почтовом сервере для ESMTP-аутентификации.

Удаление приложения

Вы можете удалить Kaspersky Security Center стандартными средствами установки и удаления приложений Microsoft Windows. Для удаления приложения запускается мастер, в результате работы которого с устройства будут удалены все компоненты приложения (включая плагины). Мастер откроет веб-страницу в вашем браузере, используемом по умолчанию, с опросом, в котором вы можете сообщить нам, почему вы решили прекратить использование Kaspersky Security Center. Если во время работы мастера вы не задали удаление папки общего доступа (KLSHARE), то после завершения всех связанных с ней задач вы можете удалить ее вручную.

После удаления приложения в системной временной папке могут оставаться файлы.

Мастер создания задачи удаления приложения предложит вам сохранить резервную копию Сервера администрирования.

При удалении приложения с операционных систем Microsoft Windows 7 и Microsoft Windows 2008 возможно преждевременное завершение работы мастера создания задачи удаления приложения. Чтобы избежать этого, отключите в операционной системе службу контроля учетных записей (UAC) и повторно запустите удаление приложения.

Об обновлении предыдущей версии Kaspersky Security Center

Этот раздел содержит информацию о том, как обновить Kaspersky Security Center с предыдущей версии. Вы можете обновить Kaspersky Security Center разными способами, в зависимости от того, был ли установлен Kaspersky Security Center локально или на узлах отказоустойчивого кластера Kaspersky Security Center.

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

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

При обновлении предыдущей версии Kaspersky Security Center все установленные плагины поддерживаемых приложений "Лаборатории Касперского" сохраняются. Плагин Сервера администрирования и плагин Агента администрирования обновляются автоматически (как для Консоли администрирования, так и для Kaspersky Security Center Web Console).

Обновление предыдущей версии Kaspersky Security Center

В следующем разделе описаны рекомендуемые этапы подготовки к обновлению: Обновление Kaspersky Security Center и управляемых приложений безопасности.

Вы можете установить Сервер администрирования версии 15.1 на устройство, на котором установлена предыдущая версия Сервера администрирования (начиная с версии 11 (11.0.0.1131b)). При обновлении до версии 15.1 все данные и параметры предыдущей версии Сервера администрирования сохраняются.

Если при установке Сервера администрирования возникли проблемы, вы можете восстановить предыдущую версию Сервера администрирования, используя созданную перед обновлением резервную копию данных Сервера.

Если в сети установлен хотя бы один Сервер администрирования новой версии, вы можете обновить другие Серверы администрирования в сети с помощью задачи удаленной установки, в которой используется инсталляционный пакет Сервера администрирования.

> Если вы развернули отказоустойчивый кластер Kaspersky Security Center, вы также можете обновить Kaspersky Security Center на его узлах.

Чтобы обновить Сервер администрирования предыдущей версии до версии 15.1:

1. Запустите исполняемый файл ksc_15.1_<номер сборки>_full_<язык локализации>.exe для версии 15.1 (вы можете загрузить этот файл с сайта "Лаборатории Касперского").

2. В открывшемся окне по ссылке **Установить Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

3. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

   - **Положения и условия настоящего Лицензионного соглашения**
   - **Политику конфиденциальности, которая описывает обработку данных**

   Установка приложения будет продолжена после установки обоих флажков. Мастер установки предложит вам создать резервную копию данных Сервера администрирования для ранних версий.

   Kaspersky Security Center поддерживает восстановление данных из резервной копии, сформированной более ранней версией Сервера администрирования.

4. Если вы хотите создать резервную копию данных Сервера администрирования, укажите это в открывшемся окне **Резервное копирование данных Сервера администрирования**.

   Резервная копия данных создается утилитой klbackup. Эта утилита входит в состав дистрибутива приложения и располагается в корне папки установки Kaspersky Security Center.

5. Установите Сервер администрирования версии 15.1, следуя указаниям мастера установки.

   Если появляется сообщение о том, что служба Kaspersky Security Center Web Console занята, в окне мастера нажмите на кнопку **Пропустить**.

   > Не рекомендуется прерывать работу мастера установки. Прерывание процесса обновления на стадии установки Сервера администрирования может привести к неработоспособности новой версии Kaspersky Security Center.

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

   > Рекомендуется обновить Агент администрирования для Linux до той же версии, что и Kaspersky Security Center.

   После выполнения задачи удаленной установки версия Агента администрирования обновлена.

   Выполните следующие команды для активов с операционной системой Linux, чтобы удалить зависимости, которые больше не нужны:

   - Для активов с операционной системой Debian выполните одну из следующих команд:
     - `apt-get -y autoremove`
     - `apt -y autoremove`
   - Для активов с операционной системой RPM выполните одну из следующих команд:
     - `dnf autoremove`
     - `yum autoremove`

Обновление Kaspersky Security Center на узле отказоустойчивого кластера Kaspersky Security Center

Вы можете установить Сервер администрирования версии 15.1 на каждом узле отказоустойчивого кластера Kaspersky Security Center, на котором установлен Сервер администрирования более ранней версии (начиная с версии 13.2). При обновлении до версии 15.1 все данные и параметры предыдущей версии Сервера администрирования сохраняются.

> Если вы ранее устанавливали Kaspersky Security Center на устройства локально, вы также можете обновить Kaspersky Security Center на этих устройствах.

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

1. Выполните следующие действия на активном узле кластера:

   a. Запустите исполняемый файл ksc_15.1_<build number>_full_<language>.exe.

      Откроется окно с выбором приложений "Лаборатории Касперского" для обновления. Перейдите по ссылке **Установка Сервера администрирования Kaspersky Security Center** для запуска мастера установки Сервера администрирования. Следуйте инструкциям мастера.

   b. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

      - **Положения и условия настоящего Лицензионного соглашения**
      - **Политику конфиденциальности, которая описывает обработку данных**

      Установите оба флажка, чтобы продолжить установку.

      Если вы не принимаете Лицензионное соглашение или Политику конфиденциальности, нажмите на кнопку **Отмена** для отмены обновления.

2. Выполните на пассивном узле отказоустойчивого кластера Kaspersky Security Center те же действия, что и на активном узле.

3. Запустить кластер.

В результате вы установили Сервер администрирования последней версии на узлы отказоустойчивого кластера Kaspersky Security Center.

Обновление Kaspersky Security Center на узлах отказоустойчивого кластера Microsoft

Вы можете обновить Сервер администрирования до версии 15.1 на каждом узле отказоустойчивого кластера Microsoft, где установлен Сервер администрирования более ранней версии (начиная с версии 13.2). При обновлении до версии 15.1 все данные и параметры предыдущей версии Сервера администрирования сохраняются.

Чтобы обновить Kaspersky Security Center на узлах отказоустойчивого кластера Microsoft, выполните следующие действия на любом узле кластера:

1. Запустите исполняемый файл ksc_15.1_<build number>_full_<language>.exe.

   Откроется окно с выбором приложений "Лаборатории Касперского" для обновления. Перейдите по ссылке **Установка Сервера администрирования Kaspersky Security Center** для запуска мастера установки Сервера администрирования. Следуйте инструкциям мастера.

2. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

   - **Положения и условия настоящего Лицензионного соглашения**
   - **Политику конфиденциальности, которая описывает обработку данных**

Установите оба флажка, чтобы продолжить установку.

Если вы не принимаете Лицензионное соглашение или Политику конфиденциальности, нажмите на кнопку **Отмена** для отмены обновления.

3. В окне **Тип установки на кластер** выберите параметр **Кластер (установить на всех узлах кластера)**.

   Далее установщик настраивает и завершает обновление Сервера администрирования на всех узлах кластера. Во время обновления параметры Сервера администрирования изменить невозможно.

В результате вы установили Сервер администрирования последней версии на узлы отказоустойчивого кластера Microsoft.

Первоначальная настройка Kaspersky Security Center

В этом разделе описаны шаги, которые необходимо выполнить после установки Kaspersky Security Center для первоначальной настройки.

Руководство по усилению защиты

Руководство по усилению защиты адресовано специалистам, которые осуществляют установку и администрирование Kaspersky Security Center, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Security Center.

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

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

Руководство по усилению защиты содержит следующую информацию:

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

Перед началом работы с Сервером администрирования, Kaspersky Security Center предложит вам ознакомиться с краткой версией Руководства по усилению защиты.

Обратите внимание, что вы не можете использовать Сервер администрирования, пока не подтвердите, что ознакомились с Руководством по усилению защиты.

Чтобы прочитать Руководство по усилению защиты:

1. Откройте Консоль администрирования или Kaspersky Security Center Web Console и войдите в консоль. Консоль 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 вы можете работать с Сервером администрирования.

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

Мастер первоначальной настройки Сервера администрирования

В этом разделе представлена информация о работе мастера первоначальной настройки Сервера администрирования.

О мастере первоначальной настройки

В этом разделе представлена информация о работе мастера первоначальной настройки Сервера администрирования.

Мастер первоначальной настройки Сервера администрирования позволяет создать минимальный набор необходимых задач и политик, настроить минимум параметров, загрузить и установить плагины для управляемых приложений "Лаборатории Касперского" и создать инсталляционные пакеты для управляемых приложений "Лаборатории Касперского". В процессе работы мастера вы можете внести в приложение следующие изменения:

- Загрузить и установить плагины для управляемых приложений. После завершения работы мастера первоначальной настройки список установленных плагинов управления отображается в разделе **Дополнительно → Информация об установленных плагинах управления приложениями** в окне свойств Сервера администрирования.

- Создать инсталляционные пакеты для управляемых приложений "Лаборатории Касперского". После завершения работы мастера первоначальной настройки инсталляционные пакеты Агента администрирования для Windows и управляемых приложений "Лаборатории Касперского" отображаются в списке **Сервер администрирования → Дополнительно → Удаленная установка → Инсталляционные пакеты**.

- Добавить файлы ключей или ввести коды активации, которые можно автоматически распространять на устройства в группах администрирования. После завершения работы мастера первоначальной настройки информация о лицензионных ключах отображается в списке **Сервер администрирования → Лицензии "Лаборатории Касперского"** и в разделе **Лицензионные ключи** окна свойств Сервера администрирования.

- Настроить взаимодействие с Kaspersky Security Network (KSN).

- Настроить рассылку по электронной почте оповещений о событиях в работе Сервера администрирования и управляемых приложений (чтобы уведомление прошло успешно, на Сервере администрирования и на всех устройствах-получателях должна быть запущена служба сообщений Messenger). После завершения работы мастера первоначальной настройки параметры почтовых уведомлений отображаются в разделе **Уведомление** в окне свойств Сервера администрирования.

- Настроить параметры обновлений и закрытия уязвимостей в приложениях, установленных на устройствах.

- Сформировать политику защиты рабочих станций и серверов, а также задачи поиска вредоносного ПО, получения обновлений и резервного копирования данных для верхнего уровня иерархии управляемых устройств. После завершения работы мастера первоначальной настройки созданные задачи отображаются в списке **Сервер администрирования → Задачи**, а политики, соответствующие плагинам управляемых приложений, отображаются в списке **Сервер администрирования → Политики**.

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

В Консоли администрирования Kaspersky Security Center автоматически предлагает запустить мастер первоначальной настройки после первого запуска приложения. Вы также можете запустить мастер первоначальной настройки вручную в любое время.

Запуск мастера первоначальной настройки Сервера администрирования

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

Чтобы запустить мастер первоначальной настройки вручную:

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню узла выберите пункт **Все задачи → Мастер первоначальной настройки Сервера администрирования**.

Мастер предложит произвести первоначальную настройку Сервера администрирования. Следуйте далее указаниям мастера.

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

Шаг 1. Настройка параметров прокси-сервера

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

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

- **Адрес**

  Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.

- **Номер порта**

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

- **Не использовать прокси-сервер для локальных адресов**

  При подключении к устройствам в локальной сети не будет использоваться прокси-сервер.

- **Аутентификация на прокси-сервере**

  Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

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

- **Имя пользователя**

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

- **Пароль**

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

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

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

Шаг 2. Выбор способа активации приложения

Выберите один из следующих вариантов активации Kaspersky Security Center:

- **Введите код активации**

  Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить ключ, активирующий Kaspersky Security Center. Код активации отправляется вам на адрес электронной почты, указанный при приобретении Kaspersky Security Center.

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

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

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

  Если этот вариант не выбран, лицензионный ключ можно будет распространить на управляемые устройства позже, в папке **Лицензии "Лаборатории Касперского"** дерева консоли администрирования.

  > Если какой-либо причине не удалось выполнить активацию с помощью кода активации, вы можете активировать приложение, указав файл ключа.

- **Укажите файл ключа**

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

  Способы получения файла ключа описаны в разделе О файле ключа.

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

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

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

  Если этот вариант не выбран, лицензионный ключ можно будет распространить на управляемые устройства позже, в папке **Лицензии "Лаборатории Касперского"** дерева консоли администрирования.

- **Отложите активацию приложения**

  Приложение будет работать в режиме Базовой функциональности, без поддержки Управления мобильными устройствами и Системного администрирования.

Если вы выбрали отложенную активацию приложения, вы можете добавить лицензионный ключ позже в любое время.

Шаг 3. Выбор областей защиты и операционных систем

Выберите области защиты и операционные системы, которые используются в вашей сети. При выборе этих параметров вы указываете фильтры для плагинов управления приложениями и дистрибутивов на серверах "Лаборатории Касперского", которые вы можете загрузить для установки на клиентские устройства в вашей сети. Выберите следующие параметры:

- **Области**

  Вы можете выбрать одну из следующих областей защиты:

  - **Рабочие станции**. Выберите этот параметр, если вы хотите защитить рабочие станции в вашей сети. По умолчанию выбран параметр Рабочая станция.
  - **Файловые серверы и системы хранения данных**. Выберите этот параметр, если вы хотите защитить файловые серверы в вашей сети.
  - **Мобильные устройства**. Выберите этот параметр, если вы хотите защитить мобильные устройства, принадлежащие компании или сотрудникам компании. Если вы выбрали этот параметр, но не предоставили лицензию с возможностью Управление мобильными устройствами, отобразится сообщение о необходимости предоставить лицензию с возможностью Управление мобильными устройствами. Без этой лицензии использование возможностей Управления мобильными устройствами невозможно.
  - **Виртуальные среды**. Выберите этот параметр, если вы хотите защитить виртуальные машины в вашей сети.
  - **Анти-Спам**. Выберите этот параметр, если вы хотите защитить почтовые серверы вашей организации от спама, мошенничества и доставки вредоносного ПО.

- **Операционные системы**

  Вы можете выбрать одну из следующих платформ:

  - Microsoft Windows
  - Linux
  - macOS
  - Android
  - Другие

  Информацию о поддерживаемых операционных системах см. в разделе Аппаратные и программные требования.

Можно выбрать инсталляционные пакеты приложений "Лаборатории Касперского" из списка доступных инсталляционных пакетов позднее без запуска мастера первоначальной настройки. Для упрощения поиска необходимых инсталляционных пакетов вы можете фильтровать список доступных инсталляционных пакетов по следующим критериям:

- область защиты;
- тип загружаемого программного обеспечения (дистрибутив, утилита, плагин или веб-плагин);
- версия приложения "Лаборатории Касперского";
- язык локализации приложения "Лаборатории Касперского".

Шаг 4. Выбор плагинов для управляемых приложений

Выберите плагины для управляемых приложений для установки. Отображается список плагинов, расположенных на серверах "Лаборатории Касперского". Список отфильтрован в соответствии с параметрами, выбранными на предыдущем шаге мастера. По умолчанию в полный список включены плагины всех языков. Чтобы отображался только плагин на выбранном языке, выберите язык в раскрывающемся списке **Отображать язык Консоли администрирования или**. Список плагинов включает в себя следующие столбцы:

- **Название приложения;**

  Выбраны плагины в зависимости от областей защиты и платформ, выбранных на предыдущем шаге.

- **Версия приложения.**

  В список включены плагины всех версий, размещенных на серверах "Лаборатории Касперского". По умолчанию выбраны плагины последних версий.

- **Localization language**

  По умолчанию язык локализации плагина зависит от языка Kaspersky Security Center, который вы выбрали при установке. Другие языки можно выбрать в раскрывающемся списке **Отображать язык Консоли администрирования или**.

После выбора плагинов, их установка начинается автоматически в отдельном окне. Для установки некоторых плагинов вам нужно принять условия Лицензионного соглашения. Ознакомьтесь с текстом Лицензионного соглашения, выберите параметр **Я принимаю условия Лицензионного соглашения** и нажмите на кнопку **Установить**. Если вы не согласны с условиями Лицензионного соглашения, плагин не установится.

После завершения установки, закройте окно установки.

Вы также можете выбрать плагин управления позднее без запуска мастера первоначальной настройки.

Шаг 5. Загрузка дистрибутивов и создание инсталляционных пакетов

Kaspersky Endpoint Security для Windows включает инструменты шифрования информации, хранящейся на клиентских устройствах. Чтобы загрузить дистрибутив Kaspersky Endpoint Security для Windows, действительный для нужд вашей организации, обратитесь к законодательству страны, в которой расположены клиентские устройства вашей организации.

В окне **Тип шифрования** выберите один из следующих типов шифрования:

- Strong encryption (AES256). Для этого типа шифрования используется 256-разрядный ключ.
- Lite encryption (AES56). Для этого типа шифрования используется 56-разрядный ключ.

Окно **Тип шифрования** отображается, только если в качестве области защиты выбран вариант **Рабочие станции**, а в качестве платформы – **Microsoft Windows**.

После того, как вы выбрали тип шифрования, отобразится список дистрибутивов для обоих типов шифрования. В списке выбран дистрибутив с выбранным типом шифрования. Язык дистрибутива соответствует языку Kaspersky Security Center. Если дистрибутив Kaspersky Endpoint Security для Windows для языка Kaspersky Security Center не существует, выбирается дистрибутив на английском языке.

В раскрывающемся списке **Отображать язык Консоли администрирования или** можно выбрать языки для дистрибутива.

Для дистрибутивов управляемых приложений может потребоваться установка определенной минимальной версии Kaspersky Security Center.

В списке вы можете выбрать дистрибутив любого типа шифрования, отличного от того, который вы выбрали в окне **Тип шифрования**. После того, как вы выбрали дистрибутив Kaspersky Endpoint Security для Windows, начинается загрузка дистрибутивов, соответствующих компонентам и платформам. Вы можете контролировать ход загрузки в графе **Состояние загрузки**. После завершения работы мастера первоначальной настройки инсталляционные пакеты Агента администрирования для Windows и управляемых приложений "Лаборатории Касперского" отображаются в списке **Сервер администрирования → Дополнительно → Удаленная установка → Инсталляционные пакеты**.

Чтобы завершить загрузку некоторых дистрибутивов вам нужно принять Лицензионное соглашение. При нажатии кнопки **Принять** отображается текст Лицензионного соглашения. Чтобы перейти к следующему шагу мастера, вам нужно принять положения и условия Лицензионного соглашения, а также условия Политики конфиденциальности "Лаборатории Касперского". Выберите параметры, связанные с Лицензионным соглашением и Политикой конфиденциальности "Лаборатории Касперского", и нажмите на кнопку **Принять все**. Если вы не принимаете положения и условия, загрузка пакета отменяется.

После того, как вы приняли положения и условия Лицензионного соглашения, а также условия Политики конфиденциальности "Лаборатории Касперского", загрузка дистрибутивов продолжается. После завершения загрузки отображается статус **Создан инсталляционный пакет**. В дальнейшем инсталляционные пакеты можно использовать для развертывания приложений "Лаборатории Касперского" на клиентских устройствах.

Вы можете создать инсталляционные пакеты позднее без запуска мастера первоначальной настройки. В дереве Консоли администрирования перейдите в раздел **Сервер администрирования → Дополнительно → Удаленная установка → Инсталляционные пакеты**.

Шаг 6. Настройка использования Kaspersky Security Network

Можно подключать репутационные базы Kaspersky Security Network, чтобы обеспечить более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повысить эффективность работы некоторых компонентов защиты, а также снизить вероятность ложных срабатываний.

Прочтите Положение о KSN, которое отображается в окне. Настройте параметры передачи информации о работе Kaspersky Security Center в базу знаний Kaspersky Security Network. Выберите один из следующих вариантов:

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

  Kaspersky Security Center и управляемые приложения, установленные на клиентских устройствах, в автоматическом режиме будут предоставлять информацию об их работе Kaspersky Security Network. Сотрудничество с Kaspersky Security Network обеспечивает более быстрое обновление баз данных о вирусах и угрозах, что увеличивает скорость реагирования на возникающие угрозы безопасности.

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

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

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

Если вы загрузили плагин Kaspersky Endpoint Security для Windows, отобразятся оба положения о KSN: Положение о KSN для Kaspersky Security Center и Положение о KSN для Kaspersky Endpoint Security для Windows. Положения о KSN для других управляемых приложений "Лаборатории Касперского", для которых были загружены плагины, отображаются в отдельных окнах и каждое из них необходимо принять (или отклонить) отдельно.

Настроить доступ Сервера администрирования к Kaspersky Security Network (KSN) можно также далее в окне свойств Сервера администрирования в Консоли администрирования.

Шаг 7. Настройка параметров отправки уведомлений по электронной почте

Настройте параметры отправки уведомлений о событиях, регистрируемых при работе приложений "Лаборатории Касперского" на управляемых устройствах. Эти параметры будут использоваться в качестве значений по умолчанию для Сервера администрирования.

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

- **Получатели (адреса электронной почты)**

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

- **SMTP-серверы**

  Адрес или адреса почтовых серверов вашей организации.

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

  - IPv4-адрес или IPv6-адрес;
  - Имя устройства в сети Windows (NetBIOS-имя);
  - DNS-имя SMTP-сервера.

- **Порт SMTP-сервера**

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

- **Использовать ESMTP-аутентификацию**

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

- **Settings**

  Задайте следующие параметры:

  - **Тема** (название темы электронного письма).
  - **Адрес отправителя электронной почты.**
  - **Параметры TLS для SMTP-сервера.**

  Вы можете указать параметры TLS для SMTP-сервера:

  Вы можете отключить использование TLS, использовать TLS, если SMTP-сервер поддерживает этот протокол, или вы можете принудительно использовать только TLS. Если вы решите использовать только TLS, можно указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также, если вы решили использовать только TLS, вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

  - Выберите файл сертификата SMTP-сервера:

  Вы можете получить файл со списком сертификатов от доверенного центра сертификации и загрузить его на Сервер администрирования. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также доверенным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от доверенного центра сертификации.

  - Выберите файл сертификата клиента:

  Вы можете использовать сертификат, полученный из любого источника, например, от любого доверенного центра сертификации. Вам нужно указать сертификат и его закрытый ключ, используя один из следующих типов сертификатов:

  - Сертификат X-509:

  Укажите файл с сертификатом и файл с закрытым ключом. Вы можете загружать эти файлы в любом порядке. Когда оба файла загружены, укажите пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

  - Контейнер pkcs12:

  Вам нужно загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

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

Вы также можете настроить уведомления о событии позднее без запуска мастера первоначальной настройки.

Шаг 8. Настройка параметров управления обновлениями

Настройте параметры работы с обновлениями приложений, установленных на клиентских устройствах.

Вы можете настроить эти параметры, только если вы предоставили лицензионный ключ, который предусматривает возможности Системного администрирования.

В блоке параметров **Режим поиска и установки обновлений** вы можете выбрать один из режимов поиска и установки обновлений Kaspersky Security Center:

- **Search for required updates**

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

  По умолчанию этот вариант выбран.

- **Искать и устанавливать требующиеся обновления**

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

В блоке параметров **Службы Windows Server Update Services** вы можете выбрать источник синхронизации обновлений:

- **Использовать источники обновлений, заданные в политике домена**

  Обновления Центра обновления Windows загружаются на клиентские устройства в соответствии с параметрами политики домена. Политика Агента администрирования создается автоматически, если она не была создана ранее.

- **Использовать Сервер администрирования в роли WSUS-сервера**

  Обновления Центра обновления Windows загружаются на клиентские устройства с Сервера администрирования. Задача *Синхронизация обновлений Windows Update* и политика Агента администрирования создаются автоматически, если они не были созданы ранее.

Вы можете создать задачи *Поиск уязвимостей и требуемых обновлений* и *Установка требуемых обновлений и закрытие уязвимостей* позднее без запуска мастера первоначальной настройки. Чтобы использовать Сервер администрирования в качестве WSUS-сервера, вам нужно создать задачу *Синхронизация обновлений Windows Update* и выбрать параметр **Использовать Сервер администрирования в роли WSUS-сервера** в политике Агента администрирования.

Шаг 9. Создание первоначальной конфигурации защиты

В окне **Создание первоначальной конфигурации защиты** отображается список политик и задач, созданных автоматически. Создаются следующие политики и задачи:

- политика Агента администрирования Kaspersky Security Center;
- политики для управляемых приложений "Лаборатории Касперского", чьи плагины управления были установлены ранее;
- задача Обслуживание Сервера администрирования;
- задача Резервное копирование данных Сервера администрирования;
- задача Загрузка обновлений в хранилище Сервера администрирования;
- задача Поиск уязвимостей и требуемых обновлений;
- задача Установка обновлений.

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

Если вы загрузили и установили плагин для Kaspersky Endpoint Security для Windows версии 10 Service Pack 1 и выше, до версии 11.0.1, во время создания политик и задач, откроется окно первоначальной настройки доверенной зоны Kaspersky Endpoint Security для Windows. Приложение предложит внести в доверенную зону проверенных "Лабораторией Касперского" поставщиков, чтобы исключить их приложения из проверки для предотвращения случайной блокировки. Вы можете создать рекомендованные исключения сейчас или создать список исключений позже, выбрав в дереве консоли **Политики** → меню свойств Kaspersky Endpoint Security → **Продвинутая защита** → **Доверенная зона** → **Настройка** → **Добавить**. Список исключений проверки доступен для редактирования в любой момент дальнейшей работы с приложением.

Работа с доверенной зоной выполняется средствами приложения Kaspersky Endpoint Security для Windows. Подробные инструкции по выполнению операций и описание особенностей шифрования приведены в справке Kaspersky Endpoint Security для Windows.

Для завершения первоначальной настройки доверенной зоны и возвращения к мастеру нажмите **OK**.

Нажмите **Далее**. Кнопка станет доступна, когда все необходимые политики и задачи будут созданы.

Также можно создать необходимые задачи и политики позднее без запуска мастера первоначальной настройки.

Шаг 10. Подключение мобильных устройств

Если ранее в параметрах мастера вы включили область защиты **Мобильные устройства**, укажите параметры подключения корпоративных мобильных устройств управляемой организацией. Если вы не включили область защиты **Мобильные устройства**, этот шаг будет пропущен.

На этом шаге мастера выполните следующие действия:

- Настройте порты подключения мобильных устройств.
- Настройте параметры аутентификации Сервера администрирования.
- Создайте сертификаты или управлять ими.
- Настройте выпуск, автоматическое обновление и шифрование сертификатов общего типа.
- Создайте правила перемещения мобильных устройств.

Чтобы настроить порты подключения мобильных устройств:

1. Нажмите на кнопку **Настроить** справа от поля **Подключение мобильных устройств**.
2. В раскрывающемся списке выберите **Настроить порты**.

   Откроется окно свойств Сервера администрирования на разделе **Дополнительные порты**.
3. В разделе **Дополнительные порты** вы можете настроить параметры подключения мобильных устройств:

   - **SSL-порт для прокси-сервера активации**

     Номер SSL-порта для подключения Kaspersky Endpoint Security 10 для Windows к серверам активации "Лаборатории Касперского".

     По умолчанию используется порт 17000.

- **Открыть порт для мобильных устройств**

  Если флажок установлен, то открыт порт, по которому мобильные устройства будут подключаться к Серверу лицензирования. Вы можете задать номер порта и другие настройки в полях ниже.

  Если флажок снят, то открытого порта для подключения мобильных устройств нет, и поля **Порт для мобильных устройств** и **Порт активации мобильных клиентов** недоступны для редактирования.

  По умолчанию флажок установлен.

- **Порт для синхронизации мобильных устройств**

  Номер порта, по которому мобильные устройства будут подключаться к Серверу администрирования и обмениваться с ним информацией. По умолчанию используется порт 13292.

  Вы можете назначить другой порт, если порт 13292 используется в каких-то других целях.

- **Порт для активации мобильных устройств**

  Порт подключения Kaspersky Endpoint Security для Android к серверам активации "Лаборатории Касперского".

  По умолчанию используется порт 17100.

- **Открыть порт для устройств с защитой на уровне UEFI и устройств с KasperskyOS**

  Если флажок установлен, то устройства с защитой на уровне UEFI могут подключаться к Серверу администрирования.

  По умолчанию флажок установлен.

- **Порт для устройств с защитой на уровне UEFI и устройств с KasperskyOS**

  Вы можете изменить номер порта, если установлен флажок **Открыть порт для устройств с защитой на уровне UEFI**. По умолчанию используется порт 13294.

- **Открыть порт для Prometheus**

  Порт для запросов на включение внесенных изменений Prometheus. По умолчанию установлен порт 13296.

4. Нажмите на кнопку **OK**, чтобы сохранить изменения и вернуться к мастеру первоначальной настройки.

Вам потребуется настроить аутентификацию Сервера администрирования мобильными устройствами и аутентификацию мобильных устройств Сервером администрирования. Вы можете настроить архитектуру приложения позже, независимо от мастера первоначальной настройки.

Чтобы настроить параметры аутентификации Сервера администрирования мобильными устройствами:

1. Нажмите на кнопку **Настроить** справа от поля **Подключение мобильных устройств**.

2. В раскрывающемся списке выберите **Настроить аутентификацию**.

   Откроется окно свойств Сервера администрирования на разделе **Сертификаты**.

3. В группе параметров **Аутентификация Сервера администрирования мобильными устройствами** выберите вариант аутентификации для мобильных устройств, а в группе параметров **Аутентификация Сервера администрирования устройствами с защитой на уровне UEFI** выберите вариант аутентификации для устройств с защитой на уровне UEFI.

   Аутентификация Сервера администрирования при обмене информацией с клиентскими устройствами выполняется на основании сертификата.

По умолчанию выбрано использование сертификата, созданного при установке Сервера администрирования. При необходимости можно добавить новый сертификат.

Чтобы добавить новый сертификат (не обязательно):

1. Выберите **Другой сертификат**.

   Появится кнопка **Обзор**.

2. Нажмите на кнопку **Обзор**.

3. В появившемся окне настройте параметры сертификата:

   - **Тип сертификата**

     В раскрывающемся списке можно выбрать способ задания сертификата:

     - **X.509-сертификат**. Если выбран этот вариант, то требуется указать закрытый ключ сертификата и открытый сертификат:

       - **Закрытый ключ**. В этом поле с помощью кнопки **Выбрать** можно указать закрытый ключ сертификата в формате PKCS#8 (*.prk).

       - **Открытый ключ**. В этом поле с помощью кнопки **Выбрать** можно указать открытый ключ сертификата в формате PEM (*.cer).

     - **Контейнер PKCS#12**. При выборе этого варианта можно указать файл сертификата в формате P12 или PFX с помощью кнопки **Выбрать** в поле **Файл сертификата**.

   - Срок активации:

     - **Немедленно**

       Текущий сертификат будет заменен новым сертификатом сразу после нажатия на кнопку **ОК**.

       Ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования.

     - **Через указанный срок (сут)**

       Если выбран этот вариант, то будет сгенерирован резервный сертификат. Текущий сертификат будет заменен новым сертификатом через указанное количество дней. Дата, с которой резервный сертификат вступит в силу, отображается в разделе **Сертификаты**.

       После того как текущий сертификат будет заменен новым сертификатом, ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования.

4. Вы можете нажать на кнопку **Свойства**, чтобы просмотреть параметры выбранного сертификата Сервера администрирования.

Чтобы перевыпустить сертификат, выпущенный средствами Сервера администрирования:

1. Выберите **Сертификат выпущен средствами Сервера администрирования**.

2. Нажмите на кнопку **Перевыпустить**.

3. В открывшемся окне настройте следующие параметры:

- Адрес подключения:

  - **Оставить адрес подключения прежним**

    Адрес Сервера администрирования, к которому подключаются мобильные устройства, останется прежним.

    Этот вариант выбран по умолчанию.

  - **Изменить адрес подключения на**

    Если необходимо, чтобы мобильные устройства подключались по другому адресу, укажите в поле требуемый адрес.

    При изменении адреса подключения мобильных устройств необходимо выпустить новый сертификат. Старый сертификат будет недействительным на подключенных мобильных устройствах. Ранее подключенные устройства не смогут подключиться к Серверу администрирования и перестанут быть управляемыми.

- Срок активации:

  - **Немедленно**

    Текущий сертификат будет заменен новым сертификатом сразу после нажатия на кнопку **ОК**.

    Ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования.

  - **Через указанный срок (сут)**

    Если выбран этот вариант, то будет сгенерирован резервный сертификат. Текущий сертификат будет заменен новым сертификатом через указанное количество дней. Дата, с которой резервный сертификат вступит в силу, отображается в разделе **Сертификаты**.

    После того как текущий сертификат будет заменен новым сертификатом, ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования.

4. Нажмите на кнопку **ОК**, чтобы сохранить изменения и вернуться к окну **Сертификаты**.

5. Нажмите на кнопку **ОК**, чтобы сохранить изменения и вернуться к мастеру первоначальной настройки.

Чтобы настроить выпуск, автоматическое обновление и шифрование сертификатов общего типа для идентификации мобильных устройств Сервером администрирования:

1. Нажмите на кнопку **Настроить** справа от поля **Аутентификация мобильных устройств**.

   Откроется окно **Правила выпуска сертификатов** на разделе **Выпуск мобильных сертификатов**.

2. При необходимости настройте следующие параметры в блоке параметров **Параметры выпуска**:

   - **Срок действия сертификата, дней**

     Срок действия сертификата в днях. По умолчанию срок действия сертификата равен 365 дням. По истечении этого срока мобильное устройство не сможет подключаться к Серверу администрирования.

- **Источник сертификата**

  Выбор источника сертификатов общего типа для мобильных устройств: сертификаты выпускает Сервер администрирования или сертификаты задаются вручную.

  Вы можете изменить шаблон сертификата, если в разделе **Интеграция с PKI** настроена интеграция с инфраструктурой открытых ключей. В этом случае будут доступны следующие поля выбора шаблона:

- **Шаблон по умолчанию**

  Использование сертификата, выпущенного внешним источником сертификатов – центром сертификации – по шаблону, заданному по умолчанию.

  По умолчанию выбран этот вариант.

- **Другой шаблон**

  Выбор шаблона, на основании которого будут выпускаться сертификаты. Шаблоны сертификатов можно задать в домене. По кнопке **Обновить список** можно обновить список шаблонов сертификатов.

3. При необходимости задайте следующие параметры автоматического выпуска сертификатов в блоке параметров **Параметры автоматического обновления**:

   - **Обновлять, когда до истечения срока действия осталось (сут)**

     Количество дней до истечения срока действия текущего сертификата, за которое Сервер администрирования должен выпустить новый сертификат. Например, если в поле указано значение 4, Сервер администрирования выпустит новый сертификат за четыре дня до окончания срока действия текущего сертификата. По умолчанию указано значение 7.

   - **Автоматически перевыпускать сертификат, если это возможно**

     При наличии возможности сертификаты будут перевыпускаться автоматически. Автоматический перевыпуск недоступен, если сертификат был задан вручную. Если флажок снят, сертификаты автоматически не перевыпускаются. По умолчанию флажок снят.

   Сертификаты обновляются автоматически центром сертификации.

4. При необходимости настройте параметры расшифровки сертификатов при установке в блоке параметров **Защита паролем**.

   Выберите параметр **Запрашивать пароль при установке сертификата**, чтобы при установке сертификата на мобильное устройство у пользователя запрашивался пароль. Пароль используется только один раз, при установке сертификата на мобильное устройство.

   Пароль будет автоматически сгенерирован средствами Сервера администрирования и отправлен по указанному вами адресу электронной почты. Вы можете указать адрес электронной почты пользователя либо свой собственный, если хотите затем передать пользователю пароль другим способом.

   Вы можете указать количество символов пароля для расшифровки сертификата с помощью ползунка.

   Функция запроса пароля необходима, например, для защиты общего сертификата в автономном инсталляционном пакете Kaspersky Endpoint Security для Android. Защита паролем не позволит злоумышленнику получить доступ к общему сертификату при краже автономного инсталляционного пакета с Веб-сервера Kaspersky Security Center.

   Если параметр выключен, расшифровка сертификата при установке будет проводиться автоматически и у пользователя не будет запрашиваться пароль. По умолчанию параметр выключен.

5. Нажмите на кнопку **OK**, чтобы сохранить изменения и вернуться к окну мастера первоначальной настройки.

   Нажмите на кнопку **Отмена**, чтобы вернуться к мастеру первоначальной настройки без сохранения внесенных изменений.

Чтобы включить функцию перемещения мобильных устройств в нужную вам группу администрирования,

В поле **Автоматически перемещать мобильные устройства** выберите параметр **Создать правило перемещения мобильных устройств**.

Если параметр **Создать правило перемещения мобильных устройств** выбран, приложение автоматически создает правило перемещения, которое перемещает устройства под управлением операционных систем Android и iOS в группу **Управляемые устройства**:

- с операционными системами Android, на которых установлен Kaspersky Endpoint Security для Android и мобильный сертификат;
- с операционными система iOS, на которых установлен iOS MDM-профиль с общим сертификатом.

Если такое правило уже существует, то приложение не создает правило.

По умолчанию параметр выключен.

"Лаборатория Касперского" больше не поддерживает Kaspersky Safe Browser.

Шаг 11. Загрузка обновлений

Обновления антивирусных баз для Kaspersky Security Center и управляемых приложений "Лаборатории Касперского" загружаются автоматически. Обновления загружаются с серверов "Лаборатории Касперского".

Чтобы загружать обновления без запуска мастера первоначальной настройки, создайте и настройте задачу *Загружать обновления в хранилище Сервера администрирования*.

Шаг 12. Обнаружение устройств

В информационном окне **Опрос сети** отображается информация о статусе опроса сети Сервером администрирования.

Вы можете просмотреть обнаруженные в сети Сервером администрирования устройства и получить справку по работе с окном **Обнаружение устройств** по ссылкам в нижней части окна.

Вы можете выполнить опрос сети позднее без запуска мастера первоначальной настройки. Используйте Консоль администрирования для настройки опроса Windows-доменов, Active Directory, IP-диапазонов и IPv6-сетей.

Шаг 13. Завершение работы мастера первоначальной настройки

В окне завершения работы мастера первоначальной настройки выберите параметр **Запускает мастер удаленной установки**, если вы хотите запустить автоматическую установку антивирусных приложений и/или Агента администрирования на устройства в вашей сети.

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

Настройка подключения Консоли администрирования к Серверу администрирования

Консоль администрирования подключена к Серверу администрирования по SSL-порту TCP 13291. Этот же порт может использоваться объектами автоматизации klakaut.

Порт TCP 14000 может использоваться для подключения Консоли администрирования, точек распространения, подчиненных Серверов администрирования и объектов автоматизации утилиты klakaut, а также для получения данных с клиентских устройств.

Как правило, SSL-порт TCP 13000 могут использовать только Агент администрирования, подчиненный Сервер и главный Сервер администрирования, размещенный в демилитаризованной зоне. В некоторых случаях может быть необходимо подключение Консоли администрирования по SSL-порту 13000:

- если предпочтительно использовать один и тот же SSL-порт как для Консоли администрирования, так и для других активностей (для получения данных с клиентских устройств, подключения точек распространения, подключения подчиненных Серверов администрирования);
- если объект автоматизации утилиты klakaut подключается к Серверу администрирования не напрямую, а через точку распространения, размещенную в демилитаризованной зоне.

Чтобы разрешить подключение Консоли администрирования по порту 13000:

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск → Выполнить**.
2. Перейдите в раздел:
   - для 32-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - для 64-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. Для ключа LP_ConsoleMustUsePort13291 (DWORD) установите значение 00000000.

   По умолчанию для этого ключа указано значение 1.
4. Перезапустите службу Сервера администрирования.

В результате Консоль администрирования сможет подключаться к Серверу администрирования, используя порт 13000.

Настройка параметров доступа Сервера администрирования к интернету

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

Чтобы указать параметры доступа Сервера администрирования к интернету:

1. В дереве консоли выберите узел **Сервер администрирования**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Дополнительно → Параметры доступа к сети интернет**.
4. Выберите параметр **Использовать прокси-сервер**, если требуется использовать прокси-сервер для подключения к интернету. Если параметр выбран, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

   - **Адрес**

     Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.

   - **Номер порта**

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

   - **Не использовать прокси-сервер для локальных адресов**

     При подключении к устройствам в локальной сети не будет использоваться прокси-сервер.

   - **Аутентификация на прокси-сервере**

     Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

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

   - **Имя пользователя**

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

   - **Пароль**

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

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

Также можно настроить доступ в интернет с помощью мастера первоначальной настройки.

Подключение автономных устройств

В этом разделе описано, как подключить автономные устройства к Серверу администрирования (то есть управляемые устройства, находящиеся вне основной сети).

Сценарий: подключение автономных устройств через шлюз соединения

В этом сценарии описано, как подключить к Серверу администрирования управляемые устройства, находящиеся вне основной сети.

Предварительные требования

Сценарий имеет следующие предварительные требования:

- В сети вашей организации организована демилитаризованная зона (DMZ).
- Сервер администрирования Kaspersky Security Center развернут в корпоративной сети.

Этапы

Этот сценарий состоит из следующих этапов:

1. **Выбор клиентского устройства в демилитаризованной зоне**

   Это устройство будет использоваться в качестве шлюза соединения. Выбранное устройство должно соответствовать требованиям для шлюзов соединения.

2. **Установка Агента администрирования в роли шлюза соединения**

   Для установки Агента администрирования на выбранное устройство рекомендуем использовать локальную установку.

   По умолчанию установочный файл находится по адресу: \\<Имя Сервера>\KLSHARE\PkgInst\NetAgent_<номер версии>.

   В окне **Шлюз соединения** мастера установки Агента администрирования выберите параметр **Использовать в качестве шлюза соединения в демилитаризованной зоне**. Этот режим одновременно активирует роль шлюза соединения и предписывает Агенту администрирования ждать соединений от Сервера администрирования, а не устанавливать соединения с Сервером администрирования.

   Также вы можете установить Агент администрирования на устройство под управлением Linux и настроить Агент администрирования для работы в качестве шлюза соединения. Обратите внимание на список ограничений Агента администрирования, работающего на устройствах под управлением Linux.

3 Разрешение соединения на сетевом экране шлюза соединения

Чтобы Сервер администрирования мог подключаться к шлюзу соединения в демилитаризованной зоне, разрешите подключения к TCP-порту 13000 во всех сетевых экранах между Сервером администрирования и шлюзом соединения.

Если шлюз соединения не имеет реального IP-адреса в интернете, но вместо этого расположен за Network Address Translation (далее также NAT), настройте правило для пересылки подключений через NAT.

4 Создание группы администрирования для внешних устройств

Создайте группу внутри группы **Управляемые устройства**. Эта новая группа будет содержать внешние управляемые устройства.

5 Подключение шлюза соединения к Серверу администрирования

Настроенный вами шлюз соединения ожидает соединения от Сервера администрирования. Однако Сервер администрирования не перечисляет устройство со шлюзом соединения среди управляемых устройств. Это связано с тем, что шлюз соединения не пытался установить соединение с Сервером администрирования. Следовательно, вам потребуется особая процедура, чтобы Сервер администрирования инициировал соединение со шлюзом соединения.

Выполните следующие действия:

1. Добавьте шлюз соединения в качестве точки распространения.
2. Переместите шлюз соединения из группы **Нераспределенные устройства** в группу, которую вы создали для внешних устройств.

Шлюз соединения подключен и настроен.

6 Подключение внешних настольных устройств к Серверу администрирования

Обычно внешние настольные устройства не перемещаются внутрь периметра сети. Поэтому вам необходимо настроить их для подключения к Серверу администрирования через шлюз соединения при установке Агента администрирования.

7 Настройка обновлений для внешних настольных устройств

Если обновления приложений безопасности настроены на загрузку с Сервера администрирования, внешние устройства загружают обновления через шлюз соединения. Это имеет два недостатка:

- Это лишний трафик, занимающий пропускную способность интернет-канала компании.
- Это не обязательно самый быстрый способ получать обновления. Возможно для внешних устройств будет удобнее получать обновления с серверов обновлений "Лаборатории Касперского".

Выполните следующие действия:

1. Переместите все внешние устройства в отдельную группу администрирования, которую вы создали ранее.
2. Исключить группу с внешними устройствами из задачи обновления.
3. Создайте отдельную задачу обновления для группы с внешними устройствами.

8. **Подключение ноутбуков к Серверу администрирования**

   Иногда ноутбуки находятся внутри сети, а в другое время – вне сети. Для эффективного управления вам необходимо, чтобы они по-разному подключались к Серверу администрирования в зависимости от своего местоположения. Для эффективного использования трафика им также необходимо получать обновления из разных источников в зависимости от их местоположения.

   Вам необходимо настроить правила для автономных пользователей: профили подключения и описания сетевых расположений. Каждое правило определяет экземпляр Сервера администрирования, к которому должны подключаться ноутбуки в зависимости от их местоположения, и экземпляр Сервера администрирования, с которого они должны получать обновления.

Сценарий: подключение автономных устройств через подчиненный Сервер администрирования в демилитаризованной зоне

Если вы хотите подключить управляемые устройства, расположенные вне основной сети, к Серверу администрирования, вы можете сделать это с помощью подчиненного Сервера администрирования, расположенного в демилитаризованной зоне (DMZ).

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- В сети вашей организации организована демилитаризованная зона (DMZ).
- Сервер администрирования Kaspersky Security Center развернут во внутренней сети организации.

Этапы

Этот сценарий состоит из следующих этапов:

1. **Выбор клиентского устройства в демилитаризованной зоне**

   В демилитаризованной зоне (DMZ) выберите клиентское устройство, которое будет использоваться в качестве подчиненного Сервера администрирования.

2. **Установка Сервера администрирования Kaspersky Security Center.**

   Установите Сервер администрирования Kaspersky Security Center на этом клиентском устройстве.

3. **Создание иерархии Серверов администрирования**

   Если вы размещаете подчиненный Сервер администрирования в демилитаризованной зоне, подчиненный Сервер администрирования должен принимать подключение от главного Сервера администрирования. Для этого добавьте новый Сервер администрирования в качестве подчиненного Сервера так, чтобы главный Сервер подключался к подчиненному Серверу по порту 13000. При объединении Серверов в иерархию необходимо, чтобы порт 13291 обоих Серверов был доступен. Через порт 13291 происходит подключение Консоли администрирования к Серверу администрирования.

4. **Подключение автономных управляемых устройств к подчиненному Серверу администрирования**

   Вы можете подключить автономные устройства к Серверу администрирования в демилитаризованной зоне аналогично тому, как устанавливается соединение между Сервером администрирования и управляемыми устройствами находящимися в основной сети. Автономные устройства инициируют подключение через порт 13000.

О подключении автономных устройств

Некоторые управляемые устройства, которые всегда находятся вне основной сети (например, устройства в региональных филиалах компании; киоски, банкоматы и терминалы, установленные в различных точках продаж; устройства в домашних офисах сотрудников), не могут быть подключены к Серверу администрирования напрямую. Некоторые устройства время от времени выходят за пределы периметра сети (например, ноутбуки пользователей, которые посещают региональные филиалы или офис клиента).

Вам по-прежнему необходимо отслеживать и управлять защитой устройств вне офиса – получать актуальную информацию об их статусе защиты и поддерживать приложения безопасности на них в актуальном состоянии. Это необходимо, например, потому, что если такое устройство будет скомпрометировано, находясь вдали от основной сети, то оно может стать платформой для распространения угроз, как только подключится к основной сети. Для подключения автономных устройств к Серверу администрирования вы можете использовать два способа:

- Шлюз соединения в демилитаризованной зоне (DMZ).

  См. схему трафика данных: Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете; использование шлюза соединения.

- Сервер администрирования в демилитаризованной зоне (DMZ)

  См. схему трафика данных: Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете.

Шлюз соединения в демилитаризованной зоне

Рекомендуемый способ подключения автономных устройств к Серверу администрирования это создание демилитаризованной зоны в сети организации и установка шлюза соединения в демилитаризованной зоне. Внешние устройства будут подключаться к шлюзу соединения, а Сервер администрирования внутри сети инициирует подключение к устройствам через шлюз соединения.

По сравнению с другим способ этот является более безопасным:

- Вам не нужно открывать доступ к Серверу администрирования извне.
- Скомпрометированный шлюз соединения не представляет большого риска для безопасности сетевых устройств. Шлюз соединения ничем не управляет и не устанавливает никаких соединений.

Кроме того, шлюз соединения не требует много аппаратных ресурсов.

Однако этот способ имеет более сложный процесс настройки:

- Чтобы устройство выполняло роль шлюза соединения в демилитаризованной зоне, вам необходимо установить Агент администрирования и подключить его к Серверу администрирования особым образом.
- Вы не сможете использовать один и тот же адрес подключения к Серверу администрирования для ситуаций. С внешней стороны периметра вам нужно будет использовать не только другой адрес (адрес шлюза соединения), но и другой режим подключения: через шлюз соединения.
- Вам также необходимо определить разные параметры подключения для ноутбуков в разных месторасположениях.

Чтобы добавить шлюз соединения в ранее настроенную сеть:

1. Установите Агент администрирования в режиме шлюза соединения.
2. Переустановите Агент администрирования на устройствах, которые вы хотите подключить к вновь добавленному шлюзу соединения.

Сервер администрирования в демилитаризованной зоне (DMZ)

Другой способ это установка единого Сервера администрирования в демилитаризованной зоне.

Эта конфигурация менее безопасна, чем конфигурация первого способа. В этом случае для управления внешними ноутбуками Сервер администрирования должен принимать соединения с любого адреса из интернета. Сервер администрирования управляет всеми устройствами во внутренней сети, но из демилитаризованной зоны. Поэтому скомпрометированный Сервер может нанести огромный ущерб, несмотря на низкую вероятность такого события.

Риск значительно снижается, если Сервер администрирования в демилитаризованной зоне не управляет устройствами внутренней сети. Такая конфигурация может использоваться, например, поставщиком услуг для управления устройствами клиентов.

Вы можете использовать этот способ в следующих случаях:

- Если вы знакомы с установкой и настройкой Сервера администрирования и не хотите выполнять другую процедуру по установке и настройке шлюза соединения.
- Если вам нужно управлять большим количеством устройств. Максимальное количество устройств, которыми может управлять Сервер администрирования – 100 000 устройств, шлюз соединения может поддерживать до 10 000 устройств.

Это решение также имеет некоторые сложности:

- Серверу администрирования требуется больше аппаратных ресурсов и еще одна база данных.
- Информация об устройствах будет храниться в двух несвязанных между собой базах данных (для Сервера администрирования внутри сети и другой в демилитаризованной зоне), что усложняет контроль.
- Для управления всеми устройствами Сервер администрирования необходимо объединить в иерархию, что усложняет и контроль и управление. Экземпляр подчиненного Сервера администрирования накладывает ограничения на возможные структуры групп администрирования. Вам нужно решить, как и какие задачи и политики распространять на подчиненный Сервер администрирования.

- Настройка внешних устройств для использования Сервера администрирования в демилитаризованной зоне извне и для использования главного Сервера администрирования изнутри не проще, чем настройка подключения через шлюз.

- Высокие риски безопасности. Скомпрометированный Сервер администрирования упрощает взлом управляемых ноутбуков. Если это произойдет, хакерам просто нужно дождаться, пока один из ноутбуков вернется в корпоративную сеть, чтобы продолжить атаку на локальную сеть.

Подключение внешних настольных устройств к Серверу администрирования

Настольные устройства, которые всегда находятся вне основной сети (например, устройства в региональных филиалах компании; киоски, банкоматы и терминалы, установленные в различных точках продаж; устройства в домашних офисах сотрудников), не могут быть подключены к Серверу администрирования напрямую. Они должны быть подключены к Серверу администрирования через шлюз соединения, установленный в демилитаризованной зоне (DMZ). Такая конфигурация выполняется при установке Агента администрирования на эти устройства.

Подключение внешних настольных устройств к Серверу администрирования

1. Создание инсталляционного пакета Агента администрирования.

2. Откройте свойства созданного инсталляционного пакета, перейдите в раздел **Дополнительно** и выберите параметр **Подключаться к Серверу администрирования через шлюз соединения**.

   Параметр **Подключаться к Серверу администрирования через шлюз соединения** несовместим с параметром **Использовать в качестве шлюза соединения в демилитаризованной зоне**. Вы не можете включить оба этих параметра одновременно.

3. Укажите адрес шлюза соединения в поле **Адрес шлюза соединений**.

   Если шлюз соединения расположен за Network Address Translation (NAT) и не имеет собственного общедоступного адреса, настройте правило шлюза NAT для перенаправления соединений с общедоступного адреса на внутренний адрес шлюза соединения.

4. Создайте автономный инсталляционный пакет на основе созданного инсталляционного пакета.

5. Доставьте автономный инсталляционный пакет на целевые устройства в электронном виде или на съемном диске.

6. Установите Агент администрирования из автономного инсталляционного пакета.

К Серверу администрирования подключены внешние настольные устройства.

О профилях соединения для автономных пользователей

При работе автономных пользователей, использующих ноутбуки (далее также "устройства"), может понадобиться изменить способ подключения к Серверу администрирования или переключиться между Серверами администрирования в зависимости от текущего положения устройства в сети.

Профили подключения поддерживаются только для устройств под управлением Windows и macOS.

Использование различных адресов одного и того же Сервера администрирования

Устройства с установленным Агентом администрирования могут в разные периоды времени подключаться к Серверу администрирования как из внутренней сети организации, так и из интернета. В этой ситуации может потребоваться, чтобы Агент администрирования использовал различные адреса для подключения к Серверу администрирования: внешний адрес Сервера при подключении из интернета и внутренний адрес Сервера при подключении из внутренней сети.

Для этого в свойствах политики Агента администрирования нужно добавить профиль для подключения к Серверу администрирования из интернета. Добавьте профиль в свойствах политики (раздел **Подключения**, вложенный раздел **Профили соединений**). В окне создания профиля необходимо выключить параметр **Использовать только для получения обновлений** и выбрать параметр **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**. Если для доступа к Серверу администрирования используется шлюз соединений (например, в конфигурации Kaspersky Security Center, описанной в разделе Доступ из интернета: Агент администрирования в качестве шлюза соединения в демилитаризованной зоне), в профиле подключения следует указать адрес шлюза соединения в соответствующем поле.

Переключение между Серверами администрирования в зависимости от текущей сети

Если в организации несколько офисов с различными Серверами администрирования и между ними перемещается часть устройств с установленным Агентом администрирования, то необходимо, чтобы Агент администрирования подключался к Серверу администрирования локальной сети того офиса, в котором находится устройство.

В этом случае в свойствах политики Агента администрирования следует создать профиль подключения к Серверу администрирования для каждого из офисов, за исключением домашнего офиса, в котором расположен исходный домашний Сервер администрирования. В профилях подключения следует указать адреса соответствующих Серверов администрирования и выбрать либо выключить параметр **Использовать только для получения обновлений**:

- выбрать параметр, если требуется, чтобы Агент администрирования синхронизировался с домашним Сервером администрирования, а локальный Сервер использовался только для загрузки обновлений;
- выключить параметр, если необходимо, чтобы Агент администрирования полностью управлялся локальным Сервером администрирования.

Далее необходимо настроить условия переключения на созданные профили: не менее одного условия для каждого из офисов, исключая "домашний офис". Смысл каждого такого условия заключается в обнаружении в сетевом окружении деталей, присущих одному из офисов. Если условие становится истинным, происходит активация соответствующего профиля. Если ни одно из условий не является истинным, Агент администрирования переключается на домашний Сервер администрирования.

Создание профиля соединения для автономных пользователей

Подключение профиля Агента администрирования к Серверу администрирования доступно только для устройств под управлением операционной системы Windows и macOS.

Чтобы создать профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей:

1. В дереве консоли выберите группу администрирования для клиентских устройств, которой требуется создать профиль подключения Агента администрирования к Серверу.

2. Выполните одно из следующих действий:

   - Если вы хотите создать профиль подключения для всех устройств группы, в рабочей области группы на вкладке **Политики** выберите политику Агента администрирования. Откройте окно свойств выбранной политики.

   - Если вы хотите создать профиль подключения для выбранного устройства в составе группы, в рабочей области группы на вкладке **Устройства** выберите устройство и выполните следующие действия:

     a. Откройте окно свойств выбранного устройства.

     b. В разделе **Приложения** окна свойств устройства выберите Агент администрирования.

     c. Откройте окно свойств Агента администрирования.

3. В окне свойств в разделе **Подключения** выберите вложенный раздел **Профили соединений**.

4. В блоке **Профили подключения к Серверу администрирования** нажмите на кнопку **Добавить**.

   По умолчанию список профилей подключения содержит профили <Офлайн-режим> и <Домашний Сервер администрирования>. Профили недоступны для изменения и удаления.

   В профиле <Офлайн-режим> не указывается Сервер для подключения. При переходе к этому профилю Агент администрирования не пытается подключиться к какому-либо Серверу, а установленные на клиентских устройствах приложения используют политики для автономных пользователей. Профиль <Офлайн-режим> применяется в условиях отключения устройств от сети.

   В профиле <Домашний Сервер администрирования> указан Сервер для подключения, который был задан при установке Агента администрирования. Профиль <Домашний Сервер администрирования> применяется в условиях, когда устройство, которое работало в другой сети, вновь подключается к домашнему Серверу администрирования.

5. В открывшемся окне **Новый профиль** настройте параметры профиля подключения:

   - **Название профиля**

     В поле ввода можно просмотреть или изменить имя профиля подключения.

- **Сервер администрирования**

  Адрес Сервера администрирования, к которому должно подключаться клиентское устройство при активации профиля.

- **Порт**

  Номер порта, по которому будет выполняться подключение.

- **SSL-порт**

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

- **Использовать SSL**

  Если этот параметр включен, подключение будет выполняться через защищенный порт (с использованием SSL-протокола).

  По умолчанию параметр включен. Чтобы ваше соединение оставалось безопасным, рекомендуется не выключать этот параметр.

- По ссылке **Настроить подключение через прокси-сервер** настройте параметры профиля подключения через прокси-сервер. Выберите параметр **Использовать прокси-сервер**, если требуется использовать прокси-сервер для подключения к интернету. Если параметр выбран, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

  - **Адрес прокси-сервера**

    Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.

  - **Номер порта**

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

  - **Аутентификация на прокси-сервере**

    Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

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

  - **Имя пользователя** (поле доступно, если выбран параметр **Аутентификация на прокси-сервере**)

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

  - **Пароль** (поле доступно, если выбран параметр **Аутентификация на прокси-сервере**)

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

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

- **Параметры шлюза соединения**

  Адрес шлюза, через который устанавливается соединение клиентских устройств с Сервером администрирования.

- **Включить автономный режим**

  Если параметр включен, при подключении через этот профиль приложения, установленные на клиентском устройстве, будут использовать профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей. В случае, если для приложения политика для автономных пользователей не определена, приложение будет использовать активную политику.

  Если параметр выключен, приложения будут использовать активные политики.

  По умолчанию параметр выключен.

- **Использовать только для получения обновлений**

  Если этот параметр включен, профиль будет использоваться только при загрузке обновлений приложениями, установленными на клиентском устройстве. Для остальных операций подключение к Серверу администрирования будет выполняться с исходными параметрами подключения, заданными при установке Агента администрирования.

  По умолчанию параметр включен.

- **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**

  Если флажок установлен, Агент администрирования подключается к Серверу администрирования, используя параметры, указанные в свойствах профиля.

  Если флажок снят, Агент администрирования подключается к Серверу используя исходные параметры, указанные при установке.

  Флажок доступен, если флажок **Использовать только для получения обновлений** снят.

  По умолчанию флажок снят.

6. Выберите параметр **Включить автономный режим, когда Сервер администрирования недоступен**, чтобы при подключении приложения, установленные на клиентском устройстве, использовали профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей, если Сервер администрирования недоступен. В случае, если для приложения политика для автономных пользователей не определена, приложение будет использовать активную политику.

В результате будет создан профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей. При подключении Агента администрирования к Серверу через этот профиль приложения, установленные на клиентском устройстве, будут использовать политики для устройств, находящиеся в автономном режиме, или политики для автономных пользователей.

О переключении Агента администрирования на другой Сервер администрирования

Исходные параметры подключения Агента администрирования к Серверу задаются при установке Агента администрирования. Для переключения Агента администрирования на другие Серверы администрирования можно использовать правила переключения. Эта функция поддерживается только для Агентов администрирования, установленных на устройствах под управлением Windows или macOS.

Правила переключения могут срабатывать при изменении следующих параметров сети:

- Адрес шлюза соединений по умолчанию.
- IP-адрес DHCP-сервера (Dynamic Host Configuration Protocol) в сети.
- DNS-суффикс подсети.

- IP-адрес DNS-сервера в сети.
- Доступность домена Windows. Этот параметр доступен только для устройств с операционными системами Windows.
- Адрес и маска подсети.
- IP-адрес DNS-сервера в сети. Этот параметр доступен только для устройств с операционными системами Windows.
- DNS-имя или NetBIOS-имя клиентского устройства.
- Доступность адреса SSL-соединения.

Если сформированы правила переключения Агента администрирования на другие Серверы администрирования, Агент реагирует на изменение параметров сети следующим образом:

- Если характеристики сети соответствуют одному из сформированных правил, Агент администрирования подключается к указанному в этом правиле Серверу администрирования. Если это задано правилом, установленные на клиентских устройствах приложения переходят на политики для автономных пользователей.
- Если ни одно из правил не выполняется, Агент администрирования возвращается к исходным параметрам подключения к Серверу администрирования, заданным при установке. Установленные на клиентских устройствах приложения возвращаются к активным политикам.
- Если Сервер администрирования недоступен, Агент администрирования использует политики для автономных пользователей.

Агент администрирования переключается на политику для автономных пользователей, только если параметр **Включить автономный режим, когда Сервер администрирования недоступен** включен в параметрах политики Агента администрирования.

Параметры подключения Агента администрирования к Серверу администрирования сохраняются в профиле подключения. В профиле подключения вы можете создавать правила перехода клиентских устройств на политики для автономных пользователей, а также настраивать профиль таким образом, чтобы он использовался только для загрузки обновлений.

Создание правила переключения Агента администрирования по сетевому местоположению

Переключение Агента администрирования доступно только для устройств под управлением операционной системы Windows и macOS.

Чтобы создать правило для переключения Агента администрирования с одного Сервера администрирования на другой при изменении характеристик сети:

1. В дереве консоли выберите группу администрирования, для устройств которой требуется создать правило переключения Агента администрирования по описанию сетевого местоположения.

2. Выполните одно из следующих действий:

   - Если вы хотите создать правило для всех устройств группы, в рабочей области группы на вкладке **Политики** выберите политику Агента администрирования. Откройте окно свойств выбранной политики.

   - Если вы хотите создать правило для выбранного устройства группы, в рабочей области группы на вкладке **Устройства** выберите устройство и выполните следующие действия:

     a. Откройте окно свойств выбранного устройства.

     b. В разделе **Приложения** окна свойств устройства выберите Агент администрирования.

     c. Откройте окно свойств Агента администрирования.

3. В открывшемся окне **Свойства** в разделе **Подключения** выберите вложенный раздел **Профили соединений**.

4. В разделе **Параметры сетевого местоположения** нажмите на кнопку **Добавить**.

5. В открывшемся окне **Новое описание** настройте параметры описания сетевого местоположения и правила переключения. Настройте следующие параметры описания сетевого местоположения:

   - **Имя описания сетевого местоположения**

     Имя описания сетевого местоположения не может превышать 255 символов и содержать специальные символы ("*<>?\/:|).

   - **Использовать профиль подключения**

     В раскрывающемся списке можно выбрать профиль подключения Агента администрирования к Серверу администрирования. Профиль будет использоваться при выполнении условий описания сетевого местоположения. Профиль подключения содержит параметры подключения Агента администрирования к Серверу администрирования и определяет переход клиентских устройств на политики для автономных пользователей. Профиль используется только для загрузки обновлений.

6. В блоке **Условия переключения** нажмите на кнопку **Добавить**, чтобы сформировать список условий описания сетевого местоположения.

   Условия правила объединяются с использованием логического оператора AND. Чтобы правило переключения по описанию сетевого местоположения сработало, все условия переключения правила должны быть выполнены.

7. В раскрывающемся списке выберите значение, соответствующее изменению характеристики сети, к которой подключено клиентское устройство:

   - **Адрес шлюза соединения по умолчанию** – изменение основного шлюза сети.

   - **Адрес DHCP-сервера** – изменение IP-адреса DHCP-сервера (Dynamic Host Configuration Protocol) в сети.

- **DNS-домен** – изменение DNS-суффикса подсети.
- **Адрес DNS-сервера** – изменение IP-адреса DNS-сервера в сети.
- **Доступность Windows-домена (только Windows)** – изменение статуса Windows-домена, к которому подключено клиентское устройство. Используйте этот параметр только для устройств под управлением Windows.
- **Подсеть** – изменение адреса и маски подсети.
- **Адрес WINS-сервера (только Windows)** – изменение IP-адреса WINS-сервера в сети. Используйте этот параметр только для устройств под управлением Windows.
- **Разрешимость имен** – у клиентского устройства изменилось NetBIOS-имя или DNS-имя.
- **Доступность адреса SSL-соединения** – клиентское устройство может или не может (в зависимости от выбранного вами параметра) установить SSL-соединение с сервером (имя:порт). Для каждого сервера вы можете дополнительно указать SSL-сертификат. В этом случае Агент администрирования проверяет сертификат сервера в дополнение к проверке возможности SSL-соединения. Если сертификаты не совпадают, соединение не устанавливается. Частота подключения – один раз в минуту.

8. В открывшемся окне укажите значение условия переключения Агента администрирования на другой Сервер администрирования. Название окна зависит от выбора значения на предыдущем шаге. Настройте следующие параметры условия переключения:

   - **Значение**

     В поле можно добавить одно или несколько значений для создаваемого условия.

   - **Соответствует хотя бы одному значению списка**

     Если выбран этот вариант, условие будет выполняться при любом из значений, указанных в списке **Значение**.

     По умолчанию выбран этот вариант.

   - **Не соответствует ни одному из значений списка**

     Если выбран этот вариант, условие будет выполняться, если его значение отсутствует в списке **Значение**.

9. В окне **Новое описание** выберите параметр **Описание активно**, чтобы включить использование нового описания сетевого местоположения.

В результате будет создано правило переключения по описанию сетевого местоположения, при выполнении условий которого Агент администрирования будет использовать для подключения к Серверу администрирования указанный в описании профиль подключения.

Описания сетевого местоположения проверяются на соответствие характеристикам сети в том порядке, в котором они представлены в списке. Если характеристики сети соответствуют нескольким описаниям, будет использоваться первое из них. Вы можете изменить порядок следования правил в списке с помощью кнопок **Вверх** () и **Вниз** ().

Уведомления о событиях

В этом разделе описано, как выбрать способ уведомления администратора о событиях на клиентских устройствах, а также как настроить параметры уведомления о событиях.

Кроме того, описано, как проверить распространение уведомлений о событиях с помощью тестового "вируса" Eicar.

Настройка параметров уведомлений о событиях

Kaspersky Security Center позволяет выбирать способ уведомления для администратора о событиях на клиентских устройствах и настраивать параметры уведомлений:

- Электронная почта. При возникновении события приложение посылает уведомление на указанные адреса электронной почты. Вы можете настроить текст уведомления.
- SMS. При возникновении события приложение посылает уведомления на указанные номера телефонов. Вы можете настроить отправку SMS оповещений с помощью почтового шлюза.
- Исполняемый файл. При возникновении события на устройстве, исполняемый файл запускается на рабочем месте администратора. С помощью исполняемого файла администратор может получать параметры произошедшего события.

Чтобы настроить параметры уведомлений о событиях на клиентских устройствах:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.
3. Перейдите по ссылке **Настроить параметры уведомлений и экспорта событий** и в раскрывающемся списке выберите значение **Настроить параметры уведомлений**.

   Откроется окно **Свойства: События**.
4. В разделе **Уведомление** выберите способ уведомления (электронная почта, SMS, исполняемый файл для запуска) и настройте параметры уведомлений:

   - **Электронная почта**

     На вкладке **Электронная почта** можно настроить уведомления о событиях по электронной почте.

     В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой.

     В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

     - IPv4-адрес или IPv6-адрес;
     - Имя устройства в сети Windows (NetBIOS-имя);
     - DNS-имя SMTP-сервера.

     В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Если вы включите параметр **Использовать DNS и MX поиск**, вы сможете использовать несколько MX-записей IP-адреса для одного и того же DNS-имени SMTP-сервера. Одно DNS-имя может иметь несколько MX-записей с различными приоритетами полученных электронных писем. Сервер администрирования пытается отправлять уведомления по электронной почте на SMTP-сервер в порядке возрастания приоритета MX-записей. По умолчанию параметр выключен.

Если вы включили параметр **Использовать DNS и MX поиск** и не разрешили использование параметров TLS, рекомендуется использовать параметры DNSSEC на вашем серверном устройстве в качестве дополнительной меры защиты при отправке уведомлений по электронной почте.

Перейдите по ссылке **Параметры**, чтобы задать дополнительные параметры:

- Тема (название темы электронного письма).
- Адрес отправителя электронной почты.
- Параметры ESMTP-аутентификации.

Вам нужно указать учетную запись для аутентификации на SMTP-сервере, если для SMTP-сервера включен параметр ESMTP-аутентификации.

- Параметры TLS для SMTP-сервера:
  - **Не использовать TLS**

    Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.
  - **Использовать TLS, если поддерживается SMTP-сервером**

    Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.
  - **Всегда использовать TLS, проверить срок действия сертификата сервера**

    Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы решите использовать значение **Всегда использовать TLS, для проверки срока действия сертификата Сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

Вы можете указать параметры TLS для SMTP-сервера:

- Выберите файл сертификата SMTP-сервера:

Вы можете получить файл со списком сертификатов от доверенного центра сертификации и загрузить его на Сервер администрирования. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также доверенным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от доверенного центра сертификации.

- Выберите файл сертификата клиента:

Вы можете использовать сертификат, полученный из любого источника, например, от любого доверенного центра сертификации. Вам нужно указать сертификат и его закрытый ключ, используя один из следующих типов сертификатов:

- Сертификат X-509:

Вам нужно указать файл с сертификатом и файл с закрытым ключом. Оба файла не зависят друг от друга. Порядок загрузки файлов не имеет значения. Когда оба файла загружены, необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

- Контейнер pkcs12:

Вам нужно загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый приложением при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив новые подстановочные параметры с подробными данными события. Список подстановочных параметров доступен по нажатию на кнопку справа от поля.

Если текст уведомления содержит знак процента (%), его нужно указать два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

Нажмите на кнопку **Отправить тестовое сообщение** можно проверить правильность настройки сообщений. Приложение отправляет тестовые сообщения на указанные адреса электронной почты.

- SMS

На вкладке **SMS** можно настроить отправку SMS-уведомлений о различных событиях на мобильный телефон. SMS-сообщения отправляются через почтовый шлюз.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой. Уведомления доставляются на телефоны, номера которых связаны с указанными адресами электронной почты.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес;
- Имя устройства в сети Windows (NetBIOS-имя);
- DNS-имя SMTP-сервера.

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Перейдите по ссылке **Параметры**, чтобы задать дополнительные параметры:

- Тема (название темы электронного письма).
- Адрес отправителя электронной почты.
- Параметры ESMTP-аутентификации.

Если необходимо, вы можете указать учетную запись для аутентификации на SMTP-сервере, если для SMTP-сервера включен параметр ESMTP-аутентификации.

- Параметры TLS для SMTP-сервера

Вы можете отключить использование TLS, использовать TLS, если SMTP-сервер поддерживает этот протокол, или вы можете принудительно использовать только TLS. Если вы решите использовать только TLS, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также, если вы решили использовать только TLS, вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

- Выберите файл сертификата SMTP-сервера

Вы можете получить файл со списком сертификатов от доверенного центра сертификации и загрузить его в Kaspersky Security Center. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также доверенным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от доверенного центра сертификации.

Вам нужно загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован. В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый приложением при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив новые подстановочные параметры с подробными данными события. Список подстановочных параметров доступен по нажатию на кнопку справа от поля.

Если текст уведомления содержит знак процента (%), его нужно указать два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

По кнопке **Отправить тестовое сообщение** проверьте, правильно ли настроены уведомления. Приложение отправляет тестовые сообщения указанным получателям.

- **Исполняемый файл для запуска**

  Если выбран этот способ уведомления, в поле ввода можно указать, какая программа будет запущена при возникновении события.

  При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

  По нажатию на кнопку **Отправить пробное сообщение** можно проверить правильно ли настроены сообщения: программа отправляет тестовые сообщения на указанные адреса электронной почты.

5. В поле **Текст уведомления** введите текст, который приложение будет отправлять при возникновении события.

   Из раскрывающегося списка, расположенного справа от текстового поля, можно добавлять в сообщение подстановочные параметры с деталями события (например, описание события, время возникновения и прочее).

Если текст уведомления содержит символ %, нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

6. По кнопке **Отправить тестовое сообщение** проверьте, правильно ли настроены уведомления.

   Приложение отправляет тестовое уведомление указанному получателю.

7. Нажмите на кнопку **OK**, чтобы сохранить изменения.

В результате настроенные параметры уведомления распространяются на все события, происходящие на клиентских устройствах.

Можно изменить значения параметров уведомлений для определенных событий в разделе **Настройка событий** параметров Сервера администрирования, параметров политики или параметров приложения.

Проверка распространения уведомлений

Для проверки распространения уведомлений о событиях используется уведомление об обнаружении тестового "вируса" Eicar на клиентских устройствах.

Чтобы проверить распространение уведомлений о событиях:

1. Остановите задачу постоянной защиты файловой системы на клиентском устройстве и скопируйте тестовый "вирус" Eicar на клиентское устройство. Снова включите задачу постоянной защиты файловой системы.

2. Запустите задачу проверки клиентских устройств для группы администрирования или набора устройств, в который входит клиентское устройство с "вирусом" Eicar.

   Если задача проверки настроена верно, в процессе ее выполнения тестовый "вирус" будет обнаружен. Если параметры уведомлений настроены верно, вы получите уведомление о найденном вирусе.

   В рабочей области узла **Сервер администрирования** на вкладке **События** в выборке **Последние события** отобразится запись об обнаружении "вируса".

Тестовый "вирус" Eicar не содержит программного кода, который может навредить вашему устройству. При этом большинство приложений безопасности компаний-производителей идентифицируют его как вирус. Загрузить тестовый "вирус" можно с официального веб-сайта организации EICAR.

Уведомление о событиях с помощью исполняемого файла

Kaspersky Security Center позволяет с помощью запуска исполняемого файла уведомлять администратора о событиях на клиентских устройствах. Исполняемый файл должен содержать другой исполняемый файл с подстановочными параметрами события, которые нужно передать администратору (см. таблицу ниже).

Подстановочные параметры для описания события

Подстановочный параметр	Описание подстановочного параметра
%SEVERITY%	Уровень важности события. Возможные значения: • **Информационное сообщение** • **Предупреждение** • **Возникшая ошибка** • **Критическое**

Подстановочный параметр	Описание подстановочного параметра
%COMPUTER%	Имя устройства, на котором произошло событие. Максимальная длина имени устройства равна 256 символов.
%DOMAIN%	Имя домена устройства, на котором произошло событие.
%EVENT%	Имя типа события. Максимальная длина названия типа события равна 50 символов.
%DESCR%	Описание события. Максимальная длина описания равна 1000 символов.
%RISE_TIME%	Время создания события.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Название задачи. Максимальная длина названия задачи равна 100 символов.
%KL_PRODUCT%	Название приложения.
%KL_VERSION%	Номер версии приложения.
%KLCSAK_EVENT_SEVERITY_NUM%	Код уровня важности события. Возможные значения: • 1 – **Информационное сообщение**. • 2 – **Предупреждение**. • 3 – **Сбой**. • 4 – **Критическое**.
%HOST_IP%	IP-адрес устройства, на котором произошло событие.
%HOST_CONN_IP%	IP-адрес соединения устройства, на котором произошло событие.

Пример:
Для уведомления о событии используется исполняемый файл (например, script1.bat), внутри которого запускается другой исполняемый файл (например, script2.bat) с подстановочным параметром %COMPUTER%. При возникновении события на устройстве администратора будет запущен файл script1.bat, который, в свою очередь, запустит файл script2.bat с параметром %COMPUTER%. В результате администратор получит имя устройства, на котором произошло событие.

Шифрование подключения TLS

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

Kaspersky Security Center использует самоподписанные сертификаты. Дополнительная настройка для iOS-устройств не требуется. Также вы можете использовать ваши собственные сертификаты. Рекомендуется использовать сертификаты, подписанные доверенным центром сертификации.

Сервер администрирования

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

1. Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Используйте флаг SrvUseStrictSslSettings, чтобы настроить разрешенные протоколы шифрования и наборы шифрования на Сервере администрирования. Введите следующую команду:

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

   Укажите параметр <value> флага SrvUseStrictSslSettings:

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

     Наборы шифрования поддерживаемые TLS-протоколом 1.2:

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

     Наборы шифрования поддерживаемые TLS-протоколом 1.3:

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

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

     Наборы шифрования поддерживаемые TLS-протоколом 1.2:

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

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

Наборы шифрования поддерживаемые TLS-протоколом 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

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

3. Перезапустите следующие службы Kaspersky Security Center 15.1:
   - службу Сервера администрирования;
   - службу Веб-сервера;
   - службу активации прокси-сервера.

Включается шифрование трафика с помощью TLS-протокола.

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

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

1. Запустите утилиту klscflag.

   Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Введите одну из следующих команд в командной строке Windows с правами администратора:
   - Используйте эту команду, чтобы включить или выключить поддержку TLS-протокола 1.2:

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

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

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

Укажите параметр < `значение` > флага:

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

Сервер iOS MDM

Соединение между iOS-устройствами и Сервером iOS MDM зашифровано.

Чтобы настроить разрешенные протоколы шифрования и наборы шифрования на Сервере iOS MDM:

1. Откройте системный реестр клиентского устройства, на котором установлен Сервер iOS MDM, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:
   - для 32-разрядной системы:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Cor
   - для 64-разрядной системы:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSI
3. Создайте ключ с именем `StrictSslSettings`.
4. Укажите тип ключа `DWORD`.
5. Установите значение ключа:
   - `2` – включены протоколы TLS 1.0, TLS 1.1 и TLS 1.2.
   - `3` – включен только протокол TLS 1.2 (значение по умолчанию).
6. Перезапустите службу Сервера iOS MDM Kaspersky Security Center.

Настройка интерфейса

Вы можете настроить интерфейс Kaspersky Security Center:

- Отобразить и скрыть объекты в дереве консоли, рабочей области и окнах свойств объектов (папок, разделов) в зависимости от используемых функций.
- Отобразить и скрыть элементы главного окна (например, дерево консоли или стандартные меню, такие как **Действия** и **Вид**).

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

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.

2. В меню главного окна приложения выберите пункт **Вид → Настройка интерфейса**.

3. В открывшемся окне **Настройка интерфейса**, настройте отображение элементов интерфейса, используя следующие флажки:

   - **Отображать Системное администрирование**

     Если флажок установлен, в папке **Удаленная установка** отображается вложенная папка **Развертывание образов устройств**, а в папке **Хранилища** отображается вложенная папка **Оборудование**.

     По умолчанию флажок снят.

   - **Отображать шифрование и защиту данных**

     Если флажок установлен, доступно управление шифрованием данных на устройствах, подключаемых к сети. После перезапуска программы в дереве консоли отобразится папка **Шифрование и защита данных**.

     По умолчанию флажок установлен.

   - **Отображать параметры контроля рабочего места**

     Если флажок установлен, в разделе **Контроль безопасности** окна свойств политики Kaspersky Endpoint Security 10 для Windows отображаются следующие подразделы:

     - **Контроль программ**;
     - **Мониторинг уязвимостей**;
     - **Контроль устройств**;
     - **Веб-Контроль**.

     Если флажок снят, указанные выше подразделы не отображаются в разделе **Контроль безопасности**.

     По умолчанию флажок снят.

   - **Отображать Управление мобильными устройствами**

     Если флажок установлен, доступна функциональность **Управление мобильными устройствами**. После перезапуска программы в дереве консоли отобразится папка **Мобильные устройства**.

     По умолчанию флажок снят.

   - **Отображать подчиненные Серверы администрирования**

     Если флажок установлен, в дереве консоли отображаются узлы подчиненных и виртуальных Серверов администрирования в составе групп администрирования. При этом доступна функциональность, связанная с подчиненными и виртуальными Серверами администрирования (например, создание задач удаленной установки программ на подчиненные Серверы администрирования).

     По умолчанию флажок установлен.

- **Отображать разделы с параметрами безопасности**

  Если флажок установлен, в окнах свойств Сервера администрирования, групп администрирования и других объектов будет отображаться раздел **Безопасность**. Это позволит предоставлять пользователям и группам пользователей права на работу с объектами, отличные от заданных по умолчанию.

  По умолчанию флажок установлен.

4. Нажмите на кнопку **OK**.

Чтобы применить некоторые изменения, вам нужно закрыть главное окно приложения, а затем открыть его снова.

Чтобы настроить отображение элементов в главном окне приложения:

1. В меню главного окна приложения выберите **Вид** → **Настроить**.
2. В открывшемся окне **Настройка вида** настройте отображение элементов главного окна с помощью флажков.
3. Нажмите на кнопку **OK**.

Обнаружение устройств в сети

В этом разделе описаны шаги, которые вам нужно выполнить после установки Kaspersky Security Center.

Сценарий: обнаружение сетевых устройств

Вам нужно выполнить поиск устройств перед установкой приложений безопасности. Сервер администрирования получает информацию об обнаруженных устройствах и позволяет управлять устройствами с помощью политик. Регулярные опросы сети необходимы для обновления списка устройств, доступных в сети.

Прежде чем начать опрос сети, убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

Обнаружение сетевых устройств содержит следующие этапы:

1. **Обнаружение устройств**

   Мастер первоначальной настройки выполняет начальное обнаружение устройств и помогает найти сетевые устройства, такие как компьютеры, планшеты и мобильные телефоны. Вы можете также запустить обнаружение устройств вручную.

2. **Настройка расписания опросов**

   Определите, какой тип опроса вы хотите регулярно использовать. Включите требуемые типы и настройте расписание опроса. Также см. рекомендации по частоте опроса сети.

3. **Задание правил для добавления обнаруженных устройств в группы администрирования (если требуется)**

   Новые устройства появляются в сети в результате их обнаружения при опросах сети. Они автоматически попадают в группу **Нераспределенные устройства**. Можно настроить правила перемещения устройств, в соответствии с которыми устройства будут распределены в группу **Управляемые устройства**. Можно также настроить правила хранения.

   Если вы пропустили шаг 3, список новых обнаруженных устройств располагается в группе **Нераспределенные устройства**. Вы можете переместить эти устройства в группу **Управляемые устройства** вручную. Если вы вручную переместили устройства в группу **Управляемые устройства**, вы можете проанализировать информацию о каждом из устройств и решить, требуется ли переместить его в группу администрирования и в какую.

Результаты

Завершение сценария дает следующее:

- Сервер администрирования Kaspersky Security Center обнаруживает устройства в сети и предоставляет информацию о них.
- Настроены будущие опросы сети и расписание их запуска.
- Новые обнаруженные устройства распределены в соответствии с заданными правилами. Если правила не заданы, устройства остаются в группе **Нераспределенные устройства**.

Нераспределенные устройства

В этом разделе представлена информация о работе с устройствами сети организации, не входящими в группы администрирования.

Обнаружение устройств

В этом разделе описаны типы обнаружения устройств, доступные в Kaspersky Security Center, а также приведена информация об использовании каждого из них.

Во время регулярных опросов сети Сервер администрирования получает информацию о структуре сети и устройствах в сети. Данные записываются в базу данных Сервера администрирования. Сервер администрирования может проводить следующие типы опросов сети:

- **Опрос сети Windows**. Сервер администрирования может проводить два типа опросов сети Windows: быстрый и полный. При быстром опросе Сервер администрирования получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети. При полном опросе с каждого клиентского устройства запрашивается более подробная информация, например, имя операционной системы, IP-адрес, DNS-имя и NetBIOS-имя. По умолчанию включены быстрый и полный опрос. При опросе сети Windows может не удаться обнаружить устройства, например, если роутером или сетевым экраном закрыты порты UDP 137, UDP 138, TCP 139.

- **Опрос Active Directory**. Сервер администрирования получает информацию о структуре групп Active Directory, а также информацию о DNS-именах устройств, входящих в группы Active Directory. По умолчанию этот тип опроса включен. При использовании Active Directory рекомендуется использовать опрос Active Directory. В противном случае Сервер администрирования не сможет обнаружить устройства. Если используется Active Directory, но отдельные сетевые устройства не являются его членами, эти устройства не удастся обнаружить при опросе Active Directory.

- **Опрос IP-диапазонов**. Сервер администрирования опрашивает указанные IP-диапазоны с помощью ICMP-пакетов или NBNS-протоколов и получает полную информацию об устройствах, входящих в IP-диапазоны. По умолчанию этот тип опроса выключен. Не рекомендуется использовать этот тип опроса, если вы используете опрос сети Windows и/или опрос Active Directory.

- **Опрос Zeroconf**. Точка распространения выполняет опрос IPv6-сети, используя сеть с нулевой конфигурацией (далее также *Zeroconf*). По умолчанию этот тип опроса выключен. Вы можете использовать опрос Zeroconf, если точка распространения работает под управлением Linux.

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**.

Можно изменить параметры обнаружения устройств для каждого типа. Например, может потребоваться изменить расписание опроса или указать, нужно опрашивать весь лес доменов или только определенный домен.

Прежде чем начать опрос сети, убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

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

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

Просмотр и изменение параметров опроса сети Windows

Чтобы изменить параметры опроса сети Windows:

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

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

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

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

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

   - **Включить опрос сети Windows**

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

   - **Настроить расписание быстрого опроса**

     По умолчанию задан период в 15 минут.

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

     Данные, полученные при следующем опросе, полностью замещают предыдущие данные.

     Доступны следующие варианты расписания опроса сети:

     - **Каждые N дней**

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

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

     - **Каждые N минут**

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

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

- **По дням недели**

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

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

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

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

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

- **Запускать пропущенные задачи**

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

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

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

  По умолчанию параметр включен.

- **Настроить расписание полного опроса**

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

  Доступны следующие варианты расписания опроса сети:

  - **Каждые N дней**

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

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

  - **Каждые N минут**

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

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

  - **По дням недели**

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

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

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

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

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

  - **Запускать пропущенные задачи**

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

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

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

По умолчанию параметр включен.

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

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

Опрос Active Directory

Используйте опрос Active Directory, если вы используете Active Directory; в противном случае рекомендуется использовать другие типы опросов. Если используется Active Directory, но отдельные сетевые устройства не являются его членами, эти устройства не удастся обнаружить при опросе Active Directory.

Результаты опроса Active Directory хранятся на Сервере администрирования в течение 30 дней независимо от результатов последующего опроса.

Прежде чем начать опрос сети, убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

Просмотр и изменение параметров опроса Active Directory

Чтобы просмотреть и изменить параметры опроса групп Active Directory:

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

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

2. Нажмите на кнопку **Настроить параметры опроса**.

   В результате откроется окно свойств Active Directory. При необходимости настройте параметры опроса групп Active Directory:

   - **Разрешить опрос Active Directory**

     По умолчанию этот вариант выбран. Однако если Active Directory не используется, в результаты опроса ничего найдено не будет. В этом случае можно отменить выбор данного параметра.

   - **Настроить расписание опроса**

     По умолчанию период составляет один час.

     Доступны следующие варианты расписания опроса сети:

     - **Каждые N дней**

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

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

- **Каждые N минут**

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

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

- **По дням недели**

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

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

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

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

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

- **Запускать пропущенные задачи**

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

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

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

  По умолчанию параметр включен.

- **Дополнительно**

  Можно выбрать домены Active Directory для опроса:

  - Домен Active Directory, к которому относится Kaspersky Security Center.
  - Лес доменов, к которому относится Kaspersky Security Center.
  - Указанный список доменов Active Directory.

    При выборе этого параметра можно добавлять домены в область применения опроса:

    - Нажмите на кнопку **Добавить**.
    - В соответствующих полях укажите адрес доменного контроллера, а также имя и пароль учетной записи для доступа к нему.
    - Нажмите на кнопку **OK**, чтобы сохранить изменения.

    Можно выбрать адрес доменного контроллера в списке и нажать на кнопку **Изменить** или **Удалить**, чтобы изменить или удалить его.

  - Нажмите на кнопку **OK**, чтобы сохранить изменения.

Если требуется запустить опрос сети сразу, нажмите на кнопку **Опросить сейчас**.

На виртуальном Сервере администрирования просмотр и изменение параметров опроса групп Active Directory осуществляются в окне свойств точки распространения, в разделе **Обнаружение устройств**.

Опрос IP-диапазонов

Сервер администрирования опрашивает указанные IP-диапазоны с помощью ICMP-пакетов или NBNS-протоколов и получает полную информацию об устройствах, входящих в IP-диапазоны. По умолчанию этот тип опроса выключен.

Для всех устройств с операционной системой Linux в контроллере домена Microsoft Active Directory или Samba укажите `netbios name` и параметры `workgroup` в файле `/etc/samba/smb.conf`. Иначе результаты опроса могут содержать дублирующиеся устройства.

Прежде чем начать опрос сети, убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

Просмотр и изменение параметров опроса IP-диапазонов

Чтобы просмотреть и изменить параметры опроса групп IP-диапазона:

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **IP-диапазоны**.

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

2. Если вы хотите, в подпапке **IP-диапазоны** нажмите на кнопку **Добавить подсеть**, чтобы добавить IP-диапазон для опроса, а затем нажмите **OK**.

3. Нажмите на кнопку **Настроить параметры опроса**.

   Откроется окно свойств IP-диапазонов. Если требуется, можно поменять параметры опроса IP-диапазонов:

   - **Разрешить опрос IP-диапазона**

     По умолчанию этот вариант не выбран. Не рекомендуется использовать этот тип опроса, если вы используете опрос сети Windows и/или опрос Active Directory.

   - **Настроить расписание опроса**

     По умолчанию задан период в 420 минут. Данные, полученные при следующем опросе, полностью заменяют предыдущие данные.

     Доступны следующие варианты расписания опроса сети:

     - **Каждые N дней**

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

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

- **Каждые N минут**

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

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

- **По дням недели**

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

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

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

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

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

- **Запускать пропущенные задачи**

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

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

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

  По умолчанию параметр включен.

Если требуется запустить опрос сети сразу, нажмите на кнопку **Опросить сейчас**. Эта кнопка доступна, только если выбран параметр **Разрешить опрос IP-диапазона**.

На виртуальном Сервере администрирования просмотр и изменение параметров опроса IP-диапазонов осуществляются в окне свойств точки распространения, в разделе **Обнаружение устройств**. Клиентские устройства, найденные в результате опроса IP-диапазонов, отображаются в папке **Домены** виртуального Сервера.

Опрос Zeroconf

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

Точка распространения может опрашивать сети, в которых есть устройства с IPv6-адресами. В этом случае IP-диапазоны не указываются, и точка распространения опрашивает всю сеть, используя сеть с нулевой конфигурацией (далее также *Zeroconf*). Чтобы начать использовать Zeroconf, вам нужно установить утилиту avahi-browse на точке распространения.

Чтобы включить опрос Zeroconf:

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **IP-диапазоны**.

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

2. Нажмите на кнопку **Настроить параметры опроса**.

3. В открывшемся окне свойств IP-диапазонов выберите **Включить опрос с помощью технологии Zeroconf**.

После этого точка распространения начинает опрашивать вашу сеть. В этом случае указанные IP-диапазоны игнорируются.

Работа с Windows-доменами Просмотр и изменение параметров домена

Чтобы изменить параметры домена:

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **Домены**.
2. Выберите домен и откройте окно его свойств одним из следующих способов:
   - В контекстном меню домена выберите пункт **Свойства**.
   - По ссылке **Показать свойства группы**.

В открывшемся окне **Свойства: <Имя домена>** можно настроить параметры выбранного домена.

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: **Дополнительно → Обнаружение устройств → Домены**. Папка **Домены** является родительской группой. Папка содержит дочерние группы, имена которых соответствуют доменам и рабочим группам, которые были обнаружены во время опроса сети. 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 опроса сети и работают, даже если опрос сети выключен.

Чтобы настроить правила хранения нераспределенных устройств:

1. В дереве консоли в папке **Обнаружение устройств** выполните одно из следующих действий:
   - Чтобы настроить параметры родительской группы, в контекстном меню папки **Домены** выберите пункт **Свойства**.

     Откроется окно свойств родительской группы.
   - Чтобы настроить параметры дочерней группы, в контекстном меню дочерней группы выберите пункт **Свойства**.

     Откроется окно свойств дочерней группы.
2. В разделе **Устройства** укажите 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.

Ваши изменения сохранены и применены.

Работа с IP-диапазонами

Вы можете настраивать параметры существующих IP-диапазонов, а также создавать новые IP-диапазоны.

Создание IP-диапазона

Чтобы создать IP-диапазон:

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **IP-диапазоны**.
2. В контекстном меню папки выберите пункт **Новый → IP-диапазон**.
3. В открывшемся окне **Новый IP-диапазон** настройте параметры создаваемого IP-диапазона.

В результате созданный IP-диапазон появится в составе папки **IP-диапазоны**.

Просмотр и изменение параметров IP-диапазона

Чтобы изменить параметры IP-диапазона:

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **IP-диапазоны**.
2. Выберите IP-диапазон и откройте окно его свойств одним из следующих способов:
   - В контекстном меню IP-диапазона выберите пункт **Свойства**.
   - По ссылке **Показать свойства группы**.

В открывшемся окне **Свойства: <Название IP-диапазона>** можно настроить параметры выбранного IP-диапазона.

Работа с группами Active Directory. Просмотр и изменение параметров группы

Чтобы изменить параметры группы Active Directory:

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **Active Directory**.
2. Выберите группу Active Directory и откройте окно ее свойств одним из следующих способов:
   - В контекстном меню IP-диапазона выберите пункт **Свойства**.
   - По ссылке **Показать свойства группы**.

   В открывшемся окне **Свойства: <Название группы Active Directory>** можно настроить параметры выбранной группы Active Directory.

Создание правил автоматического перемещения устройств в группы администрирования

Вы можете настроить автоматическое перемещение устройств, обнаруживаемых при опросе сети организации, в группы администрирования.

Чтобы настроить правила автоматического перемещения устройств в группы администрирования:

1. В дереве консоли выберите папку **Нераспределенные устройства**.
2. В рабочей области папки нажмите на кнопку **Настроить правила**.

   Откроется окно **Свойства: Нераспределенные устройства**. Настройте правила автоматического перемещения устройств в группы администрирования в разделе **Перемещение устройств**.

На устройстве будет выполнено первое применимое правило в списке (сверху вниз в списке).

Использование динамического режима VDI на клиентских устройствах

В сети организации может быть развернута виртуальная инфраструктура с использованием временных виртуальных машин. Kaspersky Security Center обнаруживает временные виртуальные машины и добавляет данные о них в базу данных Сервера администрирования. После завершения работы пользователя с временной виртуальной машиной машина удаляется из виртуальной инфраструктуры. Однако запись об удаленной виртуальной машине может сохраниться в базе данных Сервера администрирования. Кроме того, несуществующие виртуальные машины могут отображаться в Консоли администрирования.

Чтобы избежать сохранения данных о несуществующих виртуальных машинах, в Kaspersky Security Center реализована поддержка динамического режима для Virtual Desktop Infrastructure (VDI). Администратор может включить поддержку динамического режима для VDI в свойствах инсталляционного пакета Агента администрирования, который будет установлен на временной виртуальной машине.

Во время выключения временной виртуальной машины Агент администрирования информирует Сервер администрирования о выключении. В случае успешного выключения виртуальной машины, она удаляется из списка устройств, подключенных к Серверу администрирования. Если выключение виртуальной машины выполнено некорректно и Агент администрирования не послал Серверу уведомление о выключении, используется дублирующий сценарий. Согласно этому сценарию виртуальная машина удаляется из списка устройств, подключенных к Серверу администрирования, после трех неудачных попыток синхронизации с Сервером.

Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования

Чтобы включить динамический режим VDI:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета Агента администрирования выберите пункт **Свойства**.

   Откроется окно **Свойства: Агент администрирования Kaspersky Security Center**.
3. В окне **Свойства**: **Агент администрирования Kaspersky Security Center** выберите раздел **Дополнительно**.
4. В разделе **Дополнительно** выберите параметр **Включить динамический режим для VDI**.

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

Поиск устройств, являющихся частью VDI

Чтобы найти нераспределенные устройства, являющиеся частью VDI:

1. В контекстном меню папки **Нераспределенные устройства** выберите пункт **Поиск**.

   Чтобы просмотреть список всех устройств, входящих в Virtual Desktop Infrastructure (VDI), в контекстном меню папки **Сервер администрирования** выберите пункт **Поиск**.
2. В окне **Поиск** на вкладке **Виртуальные машины** выберите **Да** в блоке параметров **Часть Virtual Desktop Infrastructure**.
3. Нажмите на кнопку **Найти**.

Отобразится список нераспределенных устройств, которые являются частью Virtual Desktop Infrastructure (VDI).

Перемещение в группу администрирования устройств, являющихся частью VDI

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

1. В рабочей области папки **Нераспределенные устройства** нажмите на кнопку **Настроить правила**.

   В результате откроется окно свойств папки **Нераспределенные устройства**.

2. В окне свойств папки **Нераспределенные устройства** в разделе **Перемещение устройств** нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.

3. В окне **Новое правило** выберите раздел **Виртуальные машины**.

4. В раскрывающемся списке **Является виртуальной машиной** выберите **Да**.

Будет создано правило перемещения устройств в группу администрирования.

Инвентаризация оборудования

В списке оборудования (**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 позволяет выполнять списание оборудования. Для этого в свойствах устройства необходимо выбрать параметр **Устройство 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 дереве консоли в папке **Хранилища** выберите вложенную папку **Оборудование**.
2. В рабочей области папки **Оборудование** по кнопке **Добавить устройство** откройте окно **Новое устройство**.

   Откроется окно **Новое устройство**.
3. В окне **Новое устройство** в раскрывающемся списке **Тип** выберите тип устройства, которое вы хотите добавить.
4. Нажмите на кнопку **ОК**.

   Откроется окно свойств устройства на разделе **Общие**.
5. В разделе **Общие** заполните поля ввода данными об устройстве. В разделе **Общие** доступны следующие параметры:

   - **Корпоративное устройство**. Установите флажок, если вы хотите присвоить устройству признак *Корпоративное*. По этому признаку можно выполнять поиск устройств в папке **Оборудование**.
   - **Устройство 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 папки **Оборудование**.

Настройка критериев определения корпоративных устройств

Чтобы настроить критерии определения корпоративных устройств:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Оборудование**.
2. В рабочей области папки **Оборудование** нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Настроить критерии определения корпоративных устройств**.

   Откроется окно свойств оборудования.

3. В окне свойств оборудования в разделе **Корпоративные устройства** выберите способ присвоения устройству признака *Корпоративное*:

   - **Вручную устанавливать для устройства признак "Корпоративное"**. Признак *Корпоративное оборудование* назначается устройству вручную в окне свойств устройства в разделе **Общие**.
   - **Автоматически устанавливать для устройства признак "Корпоративное"**. В блоке параметров **По типу устройства** укажите типы устройств, которым приложение будет автоматически присваивать признак *Корпоративное*.

     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 пользовательских полей

Чтобы настроить пользовательские поля устройств:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Оборудование**.
2. В рабочей области папки **Оборудование** нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Настроить пользовательские поля данных**.

   Откроется окно свойств оборудования.
3. В окне свойств оборудования в разделе **Пользовательские поля** нажмите на кнопку **Добавить**.

   Откроется окно **Добавить поле**.
4. В окне **Добавить поле** укажите название пользовательского поля, которое будет отображаться в свойствах оборудования.

   Вы можете создать несколько пользовательских полей с уникальными именами.
5. Нажмите на кнопку **OK**.

В результате в свойствах оборудования в разделе **Пользовательские поля** будут отображаться добавленные пользовательские поля. Вы можете использовать пользовательские поля для указания специфической информации об устройствах. Например, номер внутренней заявки на приобретение оборудования.

Лицензирование

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием Kaspersky Security Center 15.1.

События превышения лицензионного ограничения

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

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

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

О лицензировании

В этом разделе содержится информация о лицензировании приложений "Лаборатории Касперского", управляемых с помощью Kaspersky Security Center.

О лицензии

Лицензия – это ограниченное по времени право на использование Kaspersky Security Center, предоставляемое вам на условиях заключенного Лицензионного договора (Лицензионного соглашения).

Список доступных функций и срок использования приложения зависят от лицензии, по которой используется приложение.

Предусмотрены следующие типы лицензий:

- *Пробная*

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

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

  Вы можете использовать приложение по пробной лицензии только в течение одного срока пробного использования.

- *Коммерческая*

  Платная лицензия.

По истечении срока действия коммерческой лицензии приложение прекращает выполнять свои основные функции. Для продолжения работы Kaspersky Security Center вам нужно продлить срок действия коммерческой лицензии. После истечения срока действия лицензии вы не можете далее использовать приложение и должны удалить его с устройства.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить непрерывность защиты устройства от угроз компьютерной безопасности.

О Лицензионном соглашении

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

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

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

Вы можете ознакомиться с условиями Лицензионного соглашения для Kaspersky Security Center следующими способами:

- Во время установки Kaspersky Security Center.
- Прочитав документ license.txt, включенный в комплект поставки Kaspersky Security Center.
- Прочитав документ license.txt в папке установки Kaspersky Security Center.
- Загрузив файл license.txt с сайта "Лаборатории Касперского".

Вы можете ознакомиться с условиями Лицензионного соглашения для Агента администрирования для Windows, Агента администрирования для Mac и Агента администрирования для Linux следующими способами:

- При загрузке дистрибутива Агента администрирования с веб-серверов "Лаборатории Касперского".
- При установке дистрибутива Агента администрирования для Windows, Агента администрирования для Mac или Агента администрирования для Linux.
- Прочитав документ license.txt, входящий в состав дистрибутива Агента администрирования для Windows, Агента администрирования для Mac или Агента администрирования для Linux.
- Прочитав документ license.txt в папке установки Агента администрирования для Windows, Агента администрирования для Mac или Агента администрирования для Linux.
- Загрузив файл license.txt с сайта "Лаборатории Касперского".

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

О 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 файле ключа

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

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

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

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

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

- Обратиться к продавцу лицензии.
- получить файл ключа на веб-сайте "Лаборатории Касперского" на основе имеющегося кода активации.
- экспортировать файл ключа с другого Сервера администрирования.

О подписке

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

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

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

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

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

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

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

При использовании приложения по подписке Kaspersky Security Center автоматически обращается к серверу активации через определенные промежутки времени вплоть до даты окончания подписки. Это обеспечивает синхронизацию информации о подписке с сервером активации. Если доступ к серверу через системный DNS невозможен, приложение использует публичные DNS-серверы. Вы можете продлить подписку на веб-сайте поставщика услуг.

Вы можете обновить информацию о подписке вручную, не дожидаясь, когда Kaspersky Security Center получит доступ к серверу активации. Например, это может быть полезно при изменении параметров подписки.

Чтобы обновить информацию о подписке вручную:

1. В дереве консоли выберите папку **Лицензии "Лаборатории Касперского"**.
2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Синхронизировать параметры подписки с Сервером лицензирования**.

Информация о подписке обновлена на сервере активации.

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

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.

Отзыв согласия с Лицензионным соглашением

Если вы решили прекратить защиту клиентских устройств, вы можете удалить управляемые приложения "Лаборатории Касперского" и отозвать Лицензионное соглашение для этих приложений.

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

1. В дереве консоли выберите **Сервер администрирования → Дополнительно → Принятые Лицензионные соглашения**.

   Отобразится список Лицензионных соглашений, принятых при создании инсталляционных пакетов, установке обновлений или развертывании Kaspersky Security для мобильных устройств.

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

   Можно просмотреть следующие свойства Лицензионных соглашений:

   - Дата принятия Лицензионного соглашения.
   - Имя пользователя, принявшего Лицензионное соглашение.
   - Ссылка на условия Лицензионного соглашения.
   - Список объектов, на которые распространяется Лицензионное соглашение: названия инсталляционных пакетов, имена обновлений, названия мобильных приложений.

3. Нажмите на кнопку **Отозвать Лицензионное соглашение**.

   В открывшемся окне отобразится информация о том, что необходимо удалить приложение "Лаборатории Касперского", которому соответствует это Лицензионное соглашение.

4. Нажмите на кнопку, подтверждающую отзыв лицензии.

   Kaspersky Security Center проверяет, удалены ли инсталляционные пакеты, соответствующие управляемому приложению "Лаборатории Касперского", Лицензионное соглашение которого вы отзываете.

   Можно отозвать только Лицензионное соглашение для управляемого приложения "Лаборатории Касперского", для которого удален инсталляционный пакет.

Лицензионное соглашение отозвано. Оно больше не отображается в списке Лицензионных соглашений в разделе **Сервер администрирования → Дополнительно → Принятые Лицензионные соглашения**. Приложение "Лаборатории Касперского", для которого было отозвано Лицензионное соглашение, больше невозможно использовать для защиты клиентских устройств.

О предоставлении данных

Данные, передаваемые третьим сторонам

При использовании Программным обеспечением функциональности для Управления мобильными устройствами для своевременной доставки команд на устройства под управлением операционной системы Android через механизм push-уведомлений используется сервис Google Firebase Cloud Messaging. Если Пользователь настроил использование службы Google Firebase Cloud Messaging, Пользователь соглашается предоставить следующую информацию службе Google Firebase Cloud Messaging в автоматическом режиме: идентификаторы установки приложений Kaspersky Endpoint Security для Android, на которые должны быть отправлены push-уведомления.

Чтобы блокировать обмен информацией со службой Google Firebase Cloud Messaging, Пользователь должен сбросить настройки использования службы Google Firebase Cloud Messaging.

При использовании Программным обеспечением функциональности для Управления мобильными устройствами для своевременной доставки команд на устройства под управлением операционной системы iOS через механизм push-уведомлений используется сервис Apple Push Notification Service (APNs). Если Пользователь установил APNs-сертификат на сервер iOS MDM, сформировал iOS MDM-профиль с набором параметров подключения мобильных устройств iOS к Программному обеспечению и установил этот iOS MDM-профиль на мобильные устройства, Пользователь соглашается в автоматическом режиме предоставлять в сервис APNs следующую информацию:

- Токен – push-токен устройства. Сервер использует этот токен при отправке push-уведомлений на устройство.
- PushMagic – строка, которая должна быть включена в push-уведомление. Значение строки генерируется устройством.

Данные, обрабатываемые локально

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

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

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

- Информация об устройствах в сети организации получена путем опроса Windows-домена, контроллеров домена Active Directory или Samba или путем опроса IP-диапазонов. Сервер администрирования независимо получает данные, или их передает ему Агент администрирования, который выполняет роль точки распространения.
- Информация из Active Directory и Samba об организационных подразделениях, доменах, пользователях и группах. Сервер администрирования независимо получает данные, или их передает ему Агент администрирования, который выполняет роль точки распространения.

- Данные об управляемых устройствах. Агент администрирования передает от устройства Серверу администрирования перечисленные ниже данные. Пользователь вводит отображаемое имя и описание устройства в интерфейс Консоли администрирования или интерфейс Kaspersky Security Center Web Console:

  - Технические характеристики управляемого устройства и его компонентов, необходимые для идентификации устройства: отображаемое имя и описание устройства, имя и тип (для устройств, принадлежащих Windows-домену), имя устройства в среде (для устройств, принадлежащих Windows-домену), DNS-домен и DNS-имя, IPv4-адрес, IPv6-адрес, сетевое местоположение, MAC-адрес, серийный номер, тип операционной системы, является ли устройство виртуальной машиной и тип гипервизора, является ли устройство динамической виртуальной машиной как частью VDI.

  - Прочие характеристики управляемых устройств и их компонентов, необходимые для аудита управляемых устройств и для принятия решений о применимости тех или иных патчей и обновлений: состояние агента обновлений Windows (WUA), архитектура операционной системы, поставщик операционной системы, номер сборки операционной системы, идентификатор выпуска операционной системы, папка расположения операционной системы, если устройство является виртуальной машиной, то тип виртуальной машины; имя виртуального Сервера администрирования, который управляет устройствами; данные об облачном устройстве (облачный регион, VPC, облачная зона доступности, облачная подсеть, группа размещения облачного устройства).

  - Подробные данные о действиях на управляемых устройствах: дата и время последнего обновления, время, когда устройство последний раз было видимо в сети, состояние ожидания перезапуска, время включения устройства.

  - Данные об учетных записях пользователей устройств и их сеансах работы.

- Данные, полученные при запуске удаленной диагностики на управляемом устройстве: файлы трассировки, системная информация, сведения об установленных на устройстве приложениях "Лаборатории Касперского", файлы дампов, журналы событий, результаты запуска диагностических скриптов, полученные от Службы технической поддержки "Лаборатории Касперского".

- Статистику работы точки распространения, если устройство является точкой распространения. Агент администрирования передает данные от устройства на Сервер администрирования.

- Параметры точки распространения, которые Пользователь вводит в Консоли администрирования или в Kaspersky Security Center Web Console.

- Данные, необходимые для подключения мобильных устройств к Серверу администрирования: сертификат, порт для подключения мобильных устройств, адрес подключения к Серверу администрирования. Пользователь вводит данные в Консоли администрирования или Kaspersky Security Center Web Console.

- Данные о мобильных устройствах, передаваемые по протоколу iOS MDM. Данные перечисленные ниже передаются от мобильного устройства Серверу администрирования:

  - Технические характеристики мобильного устройства и его компонентов, необходимые для идентификации устройства: имя устройства, модель, название и номер сборки операционной системы, номер модели устройства, номер IMEI, UDID, MEID, серийный номер, объем памяти, версия прошивки модема, MAC-адрес Bluetooth, MAC-адрес Wi-Fi и данные SIM-карты (код ICCID как часть идентификатора SIM-карты).

  - Данные о мобильной сети, используемой мобильным устройством: тип мобильной сети, название используемой мобильной сети, название домашней мобильной сети, версия параметров оператора мобильной сети, статус голосового роуминга и роуминга данных, код страны для домашней сети, код страны пребывания, код страны используемой сети и уровень шифрования.

- Параметры безопасности мобильного устройства: использование пароля и его соответствие параметрам политики, список конфигурационных профилей и provisioning-профилей, используемых для установки сторонних приложений.

- Дата последней синхронизации с Сервером администрирования и статус управления устройством.

- Данные о приложениях "Лаборатории Касперского", установленных на устройстве. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования:

  - Название и версия приложения "Лаборатории Касперского", статус, состояние постоянной защиты, дата и время последней проверки устройства, количество обнаруженных угроз, количество объектов, для которых не удалось выполнить лечение, наличие и статус компонентов приложения, время последнего обновления и версия антивирусных баз, данные о параметрах и задачах приложения "Лаборатории Касперского", информация об активном и резервных лицензионных ключах, дата и идентификатор установки приложения.

  - Статистика работы приложения: события, связанные с изменениями статуса компонентов приложения "Лаборатории Касперского" на управляемом устройстве и с выполнением задач, инициированных компонентами приложения.

  - Состояние устройства, определенное приложением "Лаборатории Касперского".

  - Теги, передаваемые приложением "Лаборатории Касперского".

  - Набор установленных и применимых обновлений к приложению "Лаборатории Касперского".

- Данные, содержащиеся в событиях от компонентов Kaspersky Security Center и управляемых приложений "Лаборатории Касперского". Агент администрирования передает данные от устройства на Сервер администрирования.

- Данные, необходимые для интеграции Kaspersky Security Center с SIEM-системой для экспорта событий. Пользователь вводит данные в Консоли администрирования или Kaspersky Security Center Web Console.

- Настройки компонентов Kaspersky Security Center и управляемых приложений "Лаборатории Касперского", представленные в виде политик и профилей политик. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.

- Настройки задач компонентов Kaspersky Security Center и управляемых приложений "Лаборатории Касперского". Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.

- Данные, обрабатываемые функцией Системное администрирование. Агент администрирования передает от устройства Серверу администрирования перечисленные ниже данные:

  - Данные о приложениях и патчах, установленных на управляемых устройствах (Реестр приложений).

  - Информация об оборудовании, обнаруженном на управляемых устройствах (Реестр оборудования).

    Если Агент администрирования установлен на устройстве с операционной системой Windows, он отправляет на Сервер администрирования следующую информацию об аппаратном обеспечении устройства:

    - оперативная память;

    - запоминающие устройства;

- материнская плата;
- процессор;
- сетевой адаптер;
- мониторы;
- видеоадаптер;
- звуковая плата.

Если Агент администрирования установлен на устройстве с операционной системой Linux или macOS, он отправляет на Сервер администрирования следующую информацию об аппаратном обеспечении устройства, если эта информация предоставляется операционной системой:

- общий объем оперативной памяти;
- общий объем запоминающих устройств;
- материнская плата;
- процессор;
- сетевой адаптер.

- Данные об уязвимостях стороннего программного обеспечения, обнаруженных на управляемых устройствах.
- Данные об обновлениях, доступных для сторонних приложений, установленных на управляемых устройствах.
- Данные об обновлениях Microsoft, найденные функцией WSUS.
- Список обновлений Microsoft, найденных функцией WSUS, которые должны быть установлены на устройство.

- Данные, которые необходимы для загрузки обновлений на изолированный Сервер администрирования для закрытия уязвимостей в приложениях сторонних производителей на управляемых устройствах. Пользователь вводит и передает данные с помощью утилиты klscflag Сервера администрирования.
- Данные, необходимые для работы Kaspersky Security Center с облачным окружением (Amazon Web Services, Microsoft Azure, Google Cloud, Yandex Cloud). Пользователь вводит данные в Консоли администрирования или Kaspersky Security Center Web Console.
- Пользовательские категории приложений. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.
- Данные об исполняемых файлах, обнаруженных на управляемых устройствах функцией Контроль приложений. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console. Полный список данных представлен в справке соответствующего приложения.
- Данные о файлах, помещенных в резервное хранилище. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Данные о файлах, помещенных в Карантин. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Данные о файлах, запрошенных экспертами "Лаборатории Касперского" для подробного анализа. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Данные о состоянии и срабатывании правил Адаптивного контроля аномалий. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Данные о внешних устройствах (устройствах памяти, инструментах передачи информации, инструментах превращения информации в твердую копию, шинах подключения), установленных или подключенных к управляемому устройству и обнаруженных функцией Контроль устройств. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Информация о зашифрованных устройствах и статусе шифрования. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования.

- Данные об ошибках шифрования данных на устройствах, выполняемого функцией Шифрование данных приложений "Лаборатории Касперского". Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Список управляемых программируемых логических контроллеров (ПЛК). Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Данные для создания цепочки развития угроз. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Информация о попытках сотрудников организации получить доступ к облачным сервисам. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Данные, необходимые для интеграции Kaspersky Security Center со службой Kaspersky Managed Detection and Response (для Kaspersky Security Center Web Console должен быть установлен специальный плагин): токен инициации интеграции, токен интеграции и токен сеанса пользователя. Пользователь с помощью токена инициации интеграции входит в интерфейс Kaspersky Security Center Web Console. Служба Kaspersky MDR передает токен интеграции и токен сеанса пользователя через специальный плагин.

- Подробная информация о введенных кодах активации или указанных файлах ключей. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.

- Учетные записи пользователей: имя, описание, полное имя, адрес электронной почты, основной номер телефона, пароль, секретный ключ, сгенерированный Сервером администрирования, и одноразовый пароль для двухфакторной аутентификации. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.

- Данные, которые необходимы Identity and Access Manager для централизованной аутентификации и для обеспечения единого входа (SSO) между приложениями "Лаборатории Касперского", интегрированными с Kaspersky Security Center: параметры установки и конфигурации Identity и Access Manager, пользовательский сеанс Identity и Access Manager, токены Identity and Access Manager, статусы клиентских приложений и статусы серверов ресурсов. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.

- Истории ревизий объектов управления. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.

- IP-адрес устройства, на котором пользователь создал ревизию. IP-адрес определяется Сервером администрирования автоматически.

- Реестр удаленных объектов управления. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.

- Инсталляционные пакеты, созданные из файла, и параметры установки. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.

- Данные, необходимые для отображения объявлений от "Лаборатории Касперского" в Kaspersky Security Center Web Console. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.

- Данные, необходимые для работы плагинов управляемых приложений в Kaspersky Security Center Web Console и сохраняемые плагинами в базе данных Сервера администрирования в процессе повседневной работы. Описание и способы предоставления данных приведены в файлах справки соответствующего приложения.

- Настройки пользователя Kaspersky Security Center Web Console: язык локализации и тема пользовательского интерфейса, настройки отображения панели мониторинга, информации о состоянии нотификаций (прочитано/не прочитано), состояние столбцов в таблицах (скрыть/показать), прогресс прохождения режима обучения. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.

- Журнал событий Kaspersky Event Log для компонентов Kaspersky Security Center и управляемых приложений "Лаборатории Касперского". Журнал событий Kaspersky Event Log хранится на устройстве и никогда не передается на Сервер администрирования.

- Сертификат безопасного подключения управляемых устройств к компонентам Kaspersky Security Center. Пользователь вводит данные с помощью утилиты klsetsrvcert Сервера администрирования.

- Сертификаты для установки доверия к внутренним веб-ресурсам организации. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.

- Данные, необходимые для работы Kaspersky Security Center в облачных окружениях, таких как Amazon Web Services (AWS), Microsoft Azure, Google Cloud и Yandex.Cloud. Сервер администрирования получает данные от виртуальной машины, на которой он запущен.

- Информация о принятии Пользователем условий юридических соглашений с "Лабораторией Касперского".

- Данные Сервера администрирования, которые Пользователь вводит в следующих компонентах:

  - Консоль администрирования.

  - Kaspersky Security Center Web Console.

    - Терминал командной строки при использовании утилиты klscflag.
    - Компоненты, взаимодействующие с Сервером администрирования через объекты автоматизации klakaut и OpenAPI Kaspersky Security Center.
- Любые данные, которые Пользователь вводит в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.

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

- Пользователь вводит данные в интерфейс следующих компонентов:
    - Консоль администрирования.
    - Kaspersky Security Center Web Console
    - Терминал командной строки при использовании утилиты klscflag.
    - Компоненты, взаимодействующие с Сервером администрирования через объекты автоматизации klakaut и OpenAPI Kaspersky Security Center.
- Агент администрирования самостоятельно получает данные с устройства и передает на Сервер администрирования.
- Агент администрирования получает собранные управляемой программой "Лаборатории Касперского" данные и передает на Сервер администрирования. Перечни данных, обрабатываемых управляемыми приложениями "Лаборатории Касперского", приведены в справках соответствующих приложений.
- Сервер администрирования самостоятельно получает данные о сетевых устройствах, или их передает ему Агент администрирования, который выполняет роль точки распространения.
- Данные передаются с мобильного устройства на Сервер администрирования по протоколу iOS MDM.

Перечисленные данные хранятся в базе данных Сервера администрирования. Имена пользователей и пароли хранятся в зашифрованном виде.

Все перечисленные выше данные могут быть переданы "Лаборатории Касперского" только посредством файлов дампа, файлов трассировки или файлов журналов компонентов Kaspersky Security Center, включая файлы журналов, создаваемые инсталляторами и утилитами.

Файлы дампа, файлы трассировки и файлы журналов компонентов Kaspersky Security Center содержат случайные данные Сервера администрирования, Агента администрирования, Консоли администрирования, Сервера iOS MDM, Kaspersky Security Center Web Console. Эти файлы могут содержать персональные и конфиденциальные данные. Файлы дампа, файлы трассировки и файлы журналов хранятся в открытой форме на устройстве. Файлы дампа, файлы трассировки и файлы журналов не передаются в "Лабораторию Касперского" автоматически, однако, администратор может передать эти данные в "Лаборатории Касперского" вручную по запросу Службы технической поддержки для решения проблем в работе Kaspersky Security Center.

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

- код Kaspersky Security Center;
- версия Kaspersky Security Center;
- язык локализации Kaspersky Security Center;

- идентификатор лицензии;
- тип лицензии;
- признак покупки лицензии через партнера.

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

"Лаборатория Касперского" использует полученные данные в анонимной форме и только для целей общей статистики. Сводная статистика автоматически формируется из полученной исходной информации и не содержит каких-либо персональных или прочих конфиденциальных данных. При накоплении новых данных предыдущие данные уничтожаются (один раз в год). Сводная статистика хранится неограниченное время.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

Варианты лицензирования Kaspersky Security Center

Kaspersky Security Center может работать в следующих режимах:

- **Лицензия отсутствует (базовая функциональность)**

  Kaspersky Security Center работает в этом режиме до активации приложения или после истечения срока действия коммерческой лицензии. Приложение Kaspersky Security Center с поддержкой базовой функциональности Консоли администрирования поставляется в составе приложений "Лаборатории Касперского", предназначенных для защиты сети организации. Кроме того, она доступна для загрузки с веб-сайта "Лаборатории Касперского".

- **Коммерческая лицензия**

  Если вам нужна дополнительная функциональность, не входящая в базовую функциональность Консоли администрирования, вам требуется приобрести коммерческую лицензию.

  При добавлении лицензионного ключа в окне свойств Сервера администрирования убедитесь, что вы добавили лицензионный ключ, который позволяет использовать Kaspersky Security Center. Вы можете найти эту информацию на сайте "Лаборатории Касперского". На странице каждого решения есть список приложений, включенных в это решение. Сервер администрирования может принимать неподдерживаемые лицензионные ключи, например лицензионный ключ для Kaspersky Endpoint Security Cloud, но такие лицензионные ключи не предоставляют никаких новых функций, кроме базовой функциональности Консоли администрирования.

Функция или свойство	Режим работы приложения Kaspersky Security Center	
	Лицензия отсутствует	Коммерческая лицензия
Базовая функциональность Консоли администрирования Доступны следующие функции: • создание виртуальных Серверов администрирования для управления сетью удаленных офисов или организаций-клиентов; • формирование иерархии групп администрирования для управления набором устройств как единым целым; • удаленная установка приложений; • централизованная настройка параметров приложений, установленных на клиентских устройствах; • контроль состояния антивирусной безопасности организации; • управление ролями пользователей; • получение статистики и отчетов о работе приложений, а также уведомлений о критических событиях; • централизованная работа с файлами, помещенными на карантин или в резервное хранилище, а также с файлами, обработка которых отложена; • управление процессом шифрования и защиты данных; • просмотр и изменение существующих групп лицензионных приложений; • просмотр и редактирование вручную списка оборудования, обнаруженного в результате опроса сети; • просмотр списка образов операционных систем, доступных для удаленной установки.	✓	✓
Системное администрирование: базовая функциональность Для следующих задач не требуется коммерческая лицензия: • Задача *Поиск уязвимостей и требуемых обновлений*. С помощью этой задачи Kaspersky Security Center получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, установленных на управляемых устройствах. • Задача *Установка обновлений Центра обновления Windows*. Эта задача может использоваться только для установки обновлений Центра обновления Windows. Для использования этой задачи необходимо вручную указать необходимые обновления в параметрах задачи. • Задача *Закрытие уязвимостей* Задача *Закрытие уязвимостей* использует рекомендованные исправления приложений Microsoft и пользовательские исправления для приложений сторонних производителей. Чтобы использовать эту задачу, требуется вручную указать пользовательские исправления для закрытия уязвимостей, которые указаны в параметрах задачи.	✓	✓
Системное администрирование: расширенная функциональность Доступны следующие функции: • Удаленная установка обновлений программного обеспечения и закрытие уязвимостей автоматически, по заданным вами правилам. • Использование Сервера администрирования в качестве сервера служб Windows Server Update Services (WSUS) для предоставления обновлений службам Windows Update на устройствах в централизованном режиме и с заданной периодичностью.	—	✓

Функция или свойство	Режим работы приложения Kaspersky Security Center	
	Лицензия отсутствует	Коммерческая лицензия
Управление мобильными устройствами в Консоли администрирования на базе MMC Возможность Управления мобильными устройствами предназначена для управления мобильными устройствами iOS MDM и Android-устройствами. Для iOS MDM-устройств доступны следующие функции: • Добавление устройств под управление Kaspersky Security Center. • Создание и редактирование конфигурационных профилей, установка конфигурационных профилей на мобильные устройства. • Установка приложений на мобильные устройства либо с помощью App Store®, либо с помощью файлов манифеста (.plist) либо с помощью мобильных инсталляционных пакетов (.ipa). • Выполнение команд на iOS MDM-устройствах, включая блокировку мобильных устройств, сброс пароля мобильного устройства и удаление всех данных с мобильного устройства. Для Android-устройств доступны следующие функции: • Добавление устройств под управление Kaspersky Security Center. • Управление Kaspersky Endpoint Security для Android с помощью политики. • Выполнение команд на устройствах. Единицей управления для Управления мобильными устройствами является мобильное устройство. Мобильное устройство считается управляемым, как только оно подключается к Серверу мобильных устройств.	—	✓ Лицензионный ключ необходимо добавить в свойствах Сервера администрирования.
Защита мобильных устройств в Kaspersky Security Center Web Console Kaspersky Security Center Web Console предоставляет следующие возможности для управления мобильными устройствами Android и iOS: • Добавление устройств под управление Kaspersky Security Center. • Управление приложениями Kaspersky Endpoint Security для Android и Kaspersky Security для iOS с помощью политик. • Отправка команд на мобильные устройства по соответствующим протоколам и выполнение команд.	—	✓ Лицензионный ключ должен быть добавлен на каждое мобильное устройство.
Управление системами Доступны следующие функции: • Установка операционных систем и приложений. Kaspersky Security Center позволяет централизованно создавать образы операционных систем и разворачивать их на клиентских устройствах по сети, а также выполнять удаленную установку приложений "Лаборатории Касперского" или других производителей программного обеспечения. Вы можете выполнять захват образов операционных систем устройств и доставлять эти образы на Сервер администрирования. Такие образы операционных систем хранятся на Сервере администрирования в специальной папке. Снятие и создание образа операционной системы эталонного устройства выполняется с помощью задачи создания инсталляционного пакета. Вы можете использовать полученные образы для развертывания на новых устройствах в сети, на которых еще не была установлена операционная система. Для этой цели используется технология Preboot eXecution Environment (PXE). • Управление группами лицензионных приложений. • Удаленное разрешение подключения к клиентским устройствам с помощью компонента Microsoft Windows "Подключение к удаленному рабочему столу". • Удаленное подключение к клиентским устройствам с помощью совместного доступа к рабочему столу Windows. • Удаленное подключение с помощью **Kaspersky Remote Desktop Session Viewer**.	—	✓

Функция или свойство	Режим работы приложения Kaspersky Security Center	
	Лицензия отсутствует	Коммерческая лицензия
Интеграция с облачными окружениями Kaspersky Security Center не только работает с физическими устройствами, но также предоставляет возможность для работы в облачном окружении, например, с помощью мастера настройки для работы в облачном окружении. Kaspersky Security Center работает со следующими виртуальными машинами: • инстансы Amazon EC2; • виртуальные машины Microsoft Azure; • инстансы виртуальных машин Google Cloud; • виртуальные машины Yandex.Cloud.	–	✓
Экспорт событий в SIEM-системы с помощью формата Syslog По протоколу Syslog можно передавать любые события, произошедшие на Сервере администрирования Kaspersky Security Center и в приложениях "Лаборатории Касперского", установленных на управляемых устройствах. Протокол Syslog – это стандартный протокол регистрации сообщений. Вы можете использовать этот протокол для экспорта событий в любую SIEM-систему.	✓	✓

Особенности лицензирования Kaspersky Security Center и управляемых приложений

Лицензирование Сервера администрирования и управляемых приложений имеет следующие особенности:

- На Сервер администрирования можно добавить лицензионный ключ или действительный код активации для активации возможностей Системного администрирования, Управления мобильными устройствами или интеграции с SIEM-системами. Некоторые функции Kaspersky Security Center доступны только при наличии активных файлов ключей или действительных кодов активации, добавленных на Сервер администрирования.

- В хранилище Сервера администрирования вы можете добавить несколько кодов активации и файлов ключей для управляемых приложений.

Особенности лицензирования Kaspersky Security Center

Например, если вы активировали с помощью файла ключа одну из возможностей (например, Управления мобильными устройствами), но вам дополнительно потребовались другие возможности (например, Системного администрирования), в этом случае необходимо приобрести ключ, который активирует обе функциональности, и активировать этим ключом Сервер администрирования.

Особенности лицензирования управляемых приложений

Для лицензирования управляемых приложений вы можете распространить код активации или файл ключа автоматически или другим удобным для вас способом. Существуют следующие способы распространения кода активации или файла ключа:

- Автоматическое распространение

Если вы используете разные управляемые приложения и вам важно распространить определенный файл ключа или код активации на устройства, используйте другие способы распространения кода активации или файла ключа.

Kaspersky Security Center позволяет автоматически распространять имеющиеся лицензионные ключи на устройства. Например, в хранилище Сервера администрирования находится три лицензионных ключа. Для всех лицензионных ключей установлен флажок **Автоматически распространять лицензионный ключ на управляемые устройства**. На устройствах организации установлено приложение безопасности "Лаборатории Касперского", например, Kaspersky Endpoint Security для Windows. Обнаружено новое устройство, на которое необходимо распространить лицензионный ключ. Приложение определяет, что для этого устройства подходит, например, два лицензионных ключа из хранилища, лицензионный ключ *Ключ_1* и лицензионный ключ *Ключ_2*. На устройство распространяется один из подходящих лицензионных ключей. В этом случае невозможно предсказать, какой из этих двух лицензионных ключей будет распространен на данное устройство, так как автоматическое распространение лицензионных ключей не предполагает вмешательства администратора.

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

- Добавление файла ключа или кода активации в инсталляционный пакет управляемого приложения

  В случае установки управляемого приложения с помощью инсталляционного пакета вы можете указать код активации или файл ключа в инсталляционном пакете или в политике этого приложения. Лицензионный ключ распространится на управляемые устройства при очередной синхронизации устройства с Сервером администрирования.

- 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.

- Добавление кода активации или файла ключа вручную на устройства

Приложения "Лаборатории Касперского". Централизованное развертывание

В этом разделе описаны способы удаленной установки приложений "Лаборатории Касперского" и их удаления с устройств сети.

Перед началом установки приложений на клиентские устройства требуется убедиться в том, что аппаратное и программное обеспечение устройств соответствует требованиям.

Связь Сервера администрирования с клиентскими устройствами обеспечивает Агент администрирования. Поэтому его необходимо установить на каждое клиентское устройство, которое будет подключено к системе удаленного централизованного управления. На устройстве, где установлен Сервер администрирования, может использоваться только серверная версия Агента администрирования. Она входит в состав Сервера администрирования и устанавливается и удаляется вместе с ним. Устанавливать Агент администрирования на это устройство не требуется.

Установка Агента администрирования осуществляется точно так же, как и установка приложений, и может быть проведена как удаленно, так и локально. При централизованной установке приложений безопасности через Консоль администрирования вы можете установить Агент администрирования совместно с приложениями безопасности.

Агенты администрирования могут отличаться в зависимости от приложений "Лаборатории Касперского", с которыми они работают. В некоторых случаях возможна только локальная установка Агента администрирования (подробнее см. в руководствах к соответствующим приложениям). Вам нужно установить Агент администрирования на клиентское устройство только один раз.

Управление приложениями "Лаборатории Касперского" через Консоль администрирования выполняется при помощи плагинов управления. Поэтому для получения доступа к управлению приложением через Kaspersky Security Center плагин управления этого приложения должен быть установлен на рабочей станции администратора.

Вы можете выполнить удаленную установку приложений с рабочей станции администратора в главном окне приложения Kaspersky Security Center.

Для удаленной установки программного обеспечения следует создать задачу удаленной установки.

Сформированная задача удаленной установки будет запускаться на выполнение в соответствии со своим расписанием. Вы можете прервать процедуру установки, остановив выполнение задачи вручную.

Если при удаленной установке приложения возникает ошибка, убедитесь, что выполнены требования к подготовке устройства.

Вы можете отслеживать процесс установки приложений безопасности "Лаборатории Касперского" в сети с помощью отчета о развертывании.

Подробную информацию об управлении перечисленными приложениями через Kaspersky Security Center см. в руководствах к соответствующим приложениям.

Замещение приложений безопасности сторонних производителей

Для установки приложения безопасности "Лаборатории Касперского" средствами Kaspersky Security Center может потребоваться удалить приложение стороннего производителя, несовместимое с устанавливаемым приложением. Kaspersky Security Center предоставляет несколько способов удаления приложений сторонних производителей.

Удаление несовместимых приложений с помощью приложения установки

Этот параметр доступен только в Консоли администрирования на основе консоли управления Microsoft Management Console.

Метод удаления несовместимых приложений поддерживается различными типами установки. Перед установкой приложения безопасности несовместимые с ним приложения удаляются автоматически, если в окне свойств инсталляционного пакета приложений безопасности (раздел **Несовместимые приложения**) выбран параметр **Удалять несовместимые приложения автоматически**.

Удаление несовместимых приложений при настройке удаленной установки приложения

Вы можете включить параметр **Удалять несовместимые приложения автоматически** во время настройки удаленной установки приложения безопасности. В Консоли администрирования на основе консоли Microsoft Management Console (MMC) этот параметр доступен в мастере удаленной установки. В приложении Kaspersky Security Center Web Console этот параметр можно найти в мастере развертывания защиты. Если этот параметр включен, Kaspersky Security Center удаляет несовместимые приложения перед установкой приложения безопасности на управляемое устройство.

Инструкции:

- Консоль администрирования: Удаление несовместимых приложений с помощью мастера удаленной установки.
- Kaspersky Security Center Web Console: Удаление несовместимых приложений перед установкой.

Удаление несовместимых приложений с помощью отдельной задачи

Для удаления несовместимых приложений используется задача **Удаленная деинсталляция приложений**. 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.

Инструкции для Консоли администрирования: Создание задачи.

Установка приложений с помощью задачи удаленной установки

Kaspersky Security Center позволяет удаленно устанавливать приложения на устройства с помощью задач удаленной установки. Задачи создаются и назначаются устройствам с помощью мастера. Чтобы быстрее и проще назначить задачу устройствам (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**. Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

- **Назначить задачу выборке устройств**. В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать предопределенную выборку 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.

Установка приложения на выбранные устройства

Чтобы установить приложение на выбранные устройства:

1. В дереве консоли выберите папку **Задачи**.

2. Запустите мастер создания задачи по кнопке **Создать задачу**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

   В окне **Выбор типа задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** выберите тип задачи **Удаленная установка приложения**.

   В результате работы мастера создания задачи будет создана задача удаленной установки выбранного приложения для выбранного набора устройств. Созданная задача отображается в рабочей области папки **Задачи**.

3. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранное приложение будет установлено на выбранные устройства.

Установка приложения на клиентские устройства группы администрирования

Чтобы установить приложение на клиентские устройства группы администрирования:

1. Подключитесь к Серверу администрирования, под управлением которого находится нужная группа администрирования.

2. В дереве консоли выберите группу администрирования.

3. В рабочей области выберите вкладку **Задачи**.

4. Запустите мастер создания задачи по кнопке **Создать задачу**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

   В окне **Выбор типа задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** выберите тип задачи **Удаленная установка приложения**.

В результате работы мастера создания задачи будет создана групповая задача удаленной установки выбранного приложения. Созданная задача отображается в рабочей области группы администрирования, на вкладке **Задачи**.

5. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранное приложение будет установлено на клиентские устройства группы администрирования.

Установка приложения с помощью групповых политик Active Directory

Kaspersky Security Center позволяет устанавливать приложения "Лаборатории Касперского" на управляемые устройства с помощью групповых политик Active Directory. Сервер администрирования должен находится одном домене с управляемыми устройствами.

> Установка приложений с помощью групповых политик Active Directory возможна только из инсталляционных пакетов, в состав которых входит Агент администрирования.

Чтобы установить приложение с помощью групповых политик Active Directory:

1. Начните настройку установки приложения с помощью мастера удаленной установки.

2. В окне мастера удаленной установки **Определение параметров задачи удаленной установки** выберите параметр **Назначить установку инсталляционного пакета в групповых политиках Active Directory**.

3. В окне мастера удаленной установки **Выбор учетных записей для доступа к устройствам** выберите параметр **Учетная запись требуется (Агент администрирования не используется)**.

4. Добавьте учетную запись с правами администратора на устройство, на котором установлен Kaspersky Security Center, или учетную запись, входящую в доменную группу Владельцы-создатели групповой политики.

5. Предоставьте разрешения выбранной учетной записи:

   a. Перейдите в **Панель управления** → **Администрирование** и откройте **Управление групповой политикой**.

   b. Нажмите на узел с нужным доменом.

   c. Нажмите на раздел **Делегирование**.

   d. В раскрывающемся списке **Права доступа** выберите **Связанные объекты GPO**.

   e. Нажмите на кнопку **Добавить**.

   f. В открывшемся окне **Выбор пользователя, компьютера или группы** выберите необходимую учетную запись.

   g. Нажмите на кнопку **OK** чтобы закрыть окно **Выбор пользователя, компьютера или группы**.

   h. В списке **Группы и пользователи** выберите только что добавленную учетную запись и нажмите на **Дополнительно** → **Дополнительно**.

i. В списке **записей разрешений** дважды нажмите на только что добавленную учетную запись.

j. Предоставьте следующие разрешения:

- **создание объектов группы;**
- **удаление объектов группы;**
- **создание объектов контейнера групповой политики;**
- **удаление объектов контейнера групповой политики.**

k. Нажмите на кнопку **OK**, чтобы сохранить изменения.

6. Задайте другие параметры, следуя инструкциям мастера.

7. Запустите созданную задачу удаленной установки вручную или дождитесь ее запуска по расписанию.

В результате будет запущен следующий механизм удаленной установки:

1. После запуска задачи в каждом домене, которому принадлежат клиентские устройства из набора, будут созданы следующие объекты:

   - Объект групповой политики (Group policy object, GPO) с именем **Kaspersky_AK{GUID}**.
   - Группа безопасности содержит клиентские устройства, на которые распространяется задача. Эта группа безопасности содержит клиентские устройства, на которые распространяется задача. Состав группы безопасности определяет область объект групповой политики (GPO).

2. Kaspersky Security Center устанавливает выбранные приложения "Лаборатории Касперского" на клиентские устройства непосредственно из сетевой папки общего доступа приложения KLSHARE. При этом в папке установки Kaspersky Security Center будет создана вложенная вспомогательная папка, содержащая файл с расширением msi для устанавливаемого приложения.

3. При добавлении новых устройств в область действия задачи они будут добавлены в группу безопасности после следующего запуска задачи. Если в расписании задачи выбран флажок **Запускать пропущенные задачи**, устройства будут добавлены в группу безопасности сразу.

4. При удалении устройств из области действия задачи их удаление из группы безопасности произойдет при следующем запуске задачи.

5. При удалении задачи из Active Directory будут удалены объект групповой политики (GPO), ссылка на объект групповой политики (GPO) и группа безопасности, связанная с задачей.

Если вы хотите использовать другую схему установки через Active Directory, вы можете настроить параметры установки вручную. Это может потребоваться, например, в следующих случаях:

- при отсутствии у администратора антивирусной защиты прав на внесение изменений в Active Directory некоторых доменов;
- при необходимости размещения исходного дистрибутива на отдельном сетевом ресурсе;
- для привязки групповой политики к конкретным подразделениям Active Directory.

Доступны следующие варианты использования другой схемы установки через Active Directory:

- Если установку требуется осуществлять непосредственно из папки общего доступа Kaspersky Security Center, в свойствах групповой политики Active Directory следует указать файл с расширением msi, расположенный во вложенной папке exec в папке инсталляционного пакета нужного приложения.

- Если инсталляционный пакет нужно разместить на другом сетевом ресурсе, следует скопировать в него все содержимое папки exec, так как помимо файла с расширением msi в ней содержатся конфигурационные файлы, сформированные при создании инсталляционного пакета. Чтобы лицензионный ключ был установлен вместе с приложением, в эту папку следует также скопировать файл ключа.

Удаленная установка приложений на устройства с операционной системой macOS

Чтобы установить приложения на устройства с операционной системой macOS с помощью задачи удаленной установки:

1. Создайте архив, состоящий из инсталляционного пакета и установочного скрипта .sh.

2. Выключите параметр **Предварительно проверять тип операционной системы перед загрузкой** в мастере создания задачи.

Также вы можете использовать задачу **Удаленное выполнение скриптов**. В следующей статье описывается, как настроить файлы для этой задачи: Удаленная установка приложений на устройства с помощью задачи Удаленное выполнение скриптов.

Установка приложений на подчиненные Серверы администрирования

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 инсталляционного пакета нет на каком-либо из подчиненных Серверов, распространите его с помощью задачи распространения инсталляционного пакета.

3. Запустите создание задачи установки приложения на подчиненные Серверы администрирования одним из следующих способов:

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

   - Если вы хотите сформировать задачу для набора подчиненных Серверов, запустите создание задачи удаленной установки для набора устройств.

   В результате запустится мастер создания задачи удаленной установки. Следуйте далее указаниям мастера.

В окне **Выбор типа задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** в папке **Дополнительно** выберите тип задачи **Удаленная установка приложения на подчиненные Серверы 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.

В результате выполнения задачи удаленной установки выбранное приложение будет установлено на выбранные подчиненные Серверы администрирования.

Установка приложений с помощью мастера удаленной установки

Для установки приложений "Лаборатории Касперского" вы можете воспользоваться мастером удаленной установки. Мастер удаленной установки позволяет проводить удаленную установку приложений как с использованием сформированных инсталляционных пакетов, так и с использованием дистрибутивов.

Для правильной работы задачи удаленной установки на клиентском устройстве, на котором не установлен Агент администрирования, необходимо открыть следующие порты: TCP 139 and 445; UDP 137 и 138. Эти порты по умолчанию открыты на всех устройствах, включенных в домен. В случае возникновения сетевых ошибок обратитесь к Базе знаний Kaspersky Security Center.

Чтобы установить приложение на выбранные устройства с помощью мастера удаленной установки:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. В рабочей области папки выберите инсталляционный пакет приложения, которое нужно установить.
3. В контекстном меню инсталляционного пакета выберите пункт **Установить приложение**.

   Запустится мастер удаленной установки.
4. В окне **Выбор устройств для установки** можно сформировать список устройств, на которые будет установлено приложение:

   - **Установить на группу управляемых устройств**

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

   - **Выбор устройств для установки**

     Если выбран этот вариант, задача удаленной установки приложения будет создана для набора устройств. В состав набора могут входить как устройства в составе групп, так и нераспределенные устройства.
5. В окне **Определение параметров задачи удаленной установки** настройте параметры удаленной установки приложения.

В блоке параметров **Принудительно загрузить 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 Сервера администрирования**

  Если этот параметр включен, доставка файлов на клиентские устройства будет осуществляться средствами операционной системы клиентских устройств с помощью Сервера администрирования. Этот параметр можно включить, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

  По умолчанию параметр включен.

- **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.

- **Количество попыток установки**

  Если при запуске задачи удаленной установки Kaspersky Security Center не удается установить приложение на управляемое устройство за указанное в параметрах количество запусков установок, Kaspersky Security Center прекращает доставку инсталляционного пакета на это управляемое устройство и больше не запускает установку на устройстве.

  Параметр `Количество попыток установки` позволяет вам сохранить ресурсы управляемого устройства, а также уменьшить трафик (деинсталляция, запуск файла MSI и сообщения об ошибках).

Повторяющиеся попытки запуска задачи могут указывать на проблему на устройстве, которая препятствует установке. Администратор должен решить проблему в течение указанного количества попыток установки (например, выделив достаточно места на диске, удалив несовместимые приложения или изменив параметры других приложений, препятствующих установке), и перезапустить задачу (вручную или по расписанию).

Если установка не выполнена, проблема будет считаться неразрешимой и любые дальнейшие запуски считаются дорогостоящими с точки зрения нежелательного расхода ресурсов и трафика.

При создании задачи счетчик попыток устанавливается на `0`. Каждый запуск установки, который возвращает ошибку на устройстве, увеличивает показания счетчика.

Если количество попыток установки, указанное в параметрах задачи, было превышено и устройство готово к установке приложения, вы можете увеличить значение параметра `Количество попыток установки` и запустить задачу по установке приложения. Также вы можете создать другую задачу удаленной установки.

Определите, какое действие выполнять с клиентскими устройствами, управляемыми другим Сервером администрирования:

- **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.

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.

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

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

  Параметр доступен, если выбран инсталляционный пакет Агента администрирования.

  По умолчанию параметр выключен.

6. В окне **Выбор лицензионного ключа** выберите лицензионный ключ и способ его распространения:

   - **Не помещать лицензионный ключ в инсталляционный пакет (рекомендуется)**

     Если выбран этот вариант, ключ будет автоматически распространяться на те устройства, для которых он подходит:

     - если в свойствах ключа настроено автоматическое распространение;
     - если создана задача **Добавление ключа**.

   - **Поместить лицензионный ключ в инсталляционный пакет**

     Ключ распространяется на устройства вместе с инсталляционным пакетом.

     > Не рекомендуется распространять ключ таким способом, так как по умолчанию к хранилищу инсталляционных пакетов настроен общий доступ на чтение.

   Окно **Выбор лицензионного ключа** отображается, если в состав инсталляционного пакета не входит лицензионный ключ.

   Если в состав инсталляционного пакета входит лицензионный ключ, отображается окно **Свойства лицензионного ключа** с информацией о лицензионном ключе.

7. В окне **Выбор параметра перезагрузки операционной системы** определите, перезагружать ли устройства, если в ходе установки приложений на них потребуется перезагрузка операционной системы:

   - **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**

     Если выбран этот вариант, после установки программы защиты пользователю будет показано сообщение о необходимости перезагрузки устройства. По ссылке **Изменить** можно изменить текст сообщения, а также период отображения сообщения и время выполнения автоматической перезагрузки.

     По умолчанию выбран этот вариант.

   - **Принудительное закрытие приложения в заблокированных сессиях через (мин)**

     Если флажок установлен, программы в заблокированных устройствах будут принудительно закрываться перед перезагрузкой.

     По умолчанию флажок снят.

8. В окне **Выбор учетных записей для доступа к устройствам** можно добавить 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 учетная запись**. Если выбран этот вариант, укажите учетную запись пользователя, от имени которой будет запускаться инсталлятор приложения. Нажмите на кнопку **Добавить**, выберите **Локальная учетная запись** и укажите данные учетной записи пользователя.

       Вы можете указать несколько учетных записей, если ни одна из них не обладает необходимыми правами на всех устройствах, для которых назначена задача. В этом случае для запуска задачи используются последовательно, сверху вниз, все добавленные учетные записи.

     - **SSH сертификат**. Если вы хотите установить 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 поддерживает формат закрытых ключей PEM, а утилита ssh-keygen по умолчанию генерирует SSH-ключи в формате OPENSSH. Формат OPENSSH не поддерживается Kaspersky Security Center. Чтобы создать закрытый ключ в поддерживаемом формате PEM, добавьте параметр -m PEM в команду ssh-keygen. Например:

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

9. В окне **Запуск установки** нажмите на кнопку **Далее** для создания и запуска задачи удаленной установки на выбранных устройствах.

   Если в окне **Запуск установки** выбран параметр **Не запускать задачу после завершения работы мастера удаленной установки**, задача удаленной установки не будет запущена. Вы можете запустить эту задачу позже вручную. Название задачи соответствует имени инсталляционного пакета для установки приложения: **Установка <Имя инсталляционного пакета>**.

Чтобы установить приложение на устройства группы администрирования с помощью мастера удаленной установки:

1. Подключитесь к Серверу администрирования, под управлением которого находится нужная группа администрирования.

2. В дереве консоли выберите группу администрирования.

3. В рабочей области группы нажмите на кнопку **Выполнить действие** и в раскрывающемся списке выберите **Установить приложение**.

   В результате запустится мастер удаленной установки. Следуйте далее указаниям мастера.

4. На последнем шаге мастера нажмите на кнопку **Далее** для создания и запуска задачи удаленной установки на выбранных устройствах.

После завершения работы мастера удаленной установки Kaspersky Security Center выполняет следующие действия:

- Создает инсталляционный пакет для установки приложения (если он не был создан раньше). Инсталляционный пакет размещается в папке **Удаленная установка**, во вложенной папке **Инсталляционные пакеты** с именем, соответствующим названию и версии приложения. Вы можете использовать этот инсталляционный пакет для установки приложения в дальнейшем.

- Создает и запускает задачу удаленной установки для набора устройств или для группы администрирования. Сформированная задача удаленной установки размещается в папке **Задачи** или добавляется к задачам группы администрирования, для которой она была создана. Вы можете запустить эту задачу позже вручную. Название задачи соответствует имени инсталляционного пакета для установки приложения: **Установка <Имя инсталляционного пакета>**.

Работа с плагинами управления

Управление приложениями "Лаборатории Касперского" через Консоль администрирования выполняется при помощи плагинов управления. В состав каждого приложения "Лаборатории Касперского", которым можно управлять при помощи Kaspersky Security Center, входит плагин управления. С помощью плагина управления приложением в Консоли администрирования можно выполнять следующие действия:

- создавать и изменять политики приложений и их параметры, а также параметры задач для приложений;

- получать информацию о задачах приложений, событиях в работе приложений и статистику работы приложений, получаемой с клиентских устройств.

Чтобы проверить список установленных плагинов и их версии:

1. В дереве Консоли администрирования нажмите правой кнопкой мыши на **Сервер администрирования <имя_сервера>** и выберите пункт **Свойства**.

2. Выберите пункт **Дополнительно → Информация об установленных плагинах управления приложениями**.

Список установленных плагинов управления и их версий появится в правой панели.

Вы можете установить плагины для управляемых приложений при запуске мастера первоначальной настройки Сервера администрирования при начальной настройке Kaspersky Security Center. Также вы можете установить плагины управления вручную.

Чтобы установить плагин управления вручную:

1. Загрузите плагин управления программы "Лаборатории Касперского" и необходимую версию программы (например, Kaspersky Endpoint Security для Windows 12.6, 12.3) со страницы Службы технической поддержки "Лаборатории Касперского".

2. Если Консоль администрирования запущена, закройте ее.

3. Разархивируйте загруженный файл плагина и запустите файл klcfginst.msi или klcfginst.exe. Следуйте инструкциям мастера установки.

4. После завершения установки запустите Консоль администрирования и убедитесь, что плагин присутствует в списке установленных плагинов, как описано в предыдущей процедуре.

При запуске Консоли администрирования после установки плагина управления, который поддерживает мастер первоначальной настройки управляемых приложений, этот мастер запускается автоматически. Вы можете выполнить шаги мастера первоначальной настройки управляемых приложений, чтобы создать политики и задачи приложений "Лаборатории Касперского" по умолчанию. Мастер запускается автоматически только при запуске Консоли администрирования после первоначальной установки плагина или после обновления плагина управления до версии, совместимой с другой версией приложения "Лаборатории Касперского", для которого еще не созданы задачи и политики. Вы также можете запустить мастер первоначальной настройки управляемых приложений вручную.

Чтобы запустить мастер первоначальной настройки управляемых приложений вручную:

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.

2. В контекстном меню узла Сервера администрирования выберите пункт **Все задачи** → **Мастер первоначальной настройки управляемых приложений**.

3. Запустится мастер первоначальной настройки управляемых приложений. Следуйте инструкциям мастера, чтобы создать политики и задачи приложений "Лаборатории Касперского" с параметрами по умолчанию.

Чтобы удалить плагин управления:

1. Если Консоль администрирования запущена, закройте ее.

2. Откройте редактор реестра операционной системы Windows.

3. Найдите следующий ключ:

   - `HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\28\Plugins` для 32-разрядной системы.

   - `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins` для 64-разрядной системы.

   Ключ содержит установленные плагины управления. Для каждого плагина значение `DisplayName` содержит имя плагина, а значение `UninstallString` содержит команду для удаления плагина.

4. Найдите ключ плагина, который вы хотите удалить, и скопируйте его значение `UninstallString` в буфер обмена.

5. Вставьте значение в командную строку и запустите ее с правами системного администратора.

Версия плагина управления не должна быть ниже, чем версия управляемого приложения "Лаборатории Касперского". При обновлении приложения "Лаборатории Касперского" на устройствах необходимо установить плагин управления той же версии.

При открытии политики, созданной в более ранней версии плагина, вам будет предложено принять Положение о Kaspersky Security Network.

При удалении Kaspersky Security Center Web Console также удаляются все плагины управления.

Если вы откроете и сохраните политику в версии плагина, более поздней, чем версия управляемого приложения, политика будет обновлена, и вы не сможете открыть ее в плагине более ранней версии.

Просмотр отчета о развертывании защиты

Для отслеживания процесса развертывания защиты в сети можно использовать отчет о развертывании защиты.

Чтобы просмотреть отчет о развертывании защиты:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.

2. В рабочей области узла выберите вкладку **Отчеты**.

3. В рабочей области вкладки **Отчеты** выберите шаблон отчета **Просмотреть отчет о развертывании защиты**.

В рабочей области будет сформирован отчет, содержащий информацию о развертывании защиты на всех устройствах сети.

Вы можете сформировать новый отчет о развертывании защиты и указать, информацию какого типа в него следует включать:

- для группы администрирования;

- для набора устройств;

- для выборки устройств;
- для всех устройств.

В рамках Kaspersky Security Center считается, что на устройстве развернута защита в том случае, когда на нем установлено приложение безопасности и включена постоянная защита.

Удаленная деинсталляция приложений

Kaspersky Security Center позволяет удаленно деинсталлировать приложения с устройств с помощью задач удаленной деинсталляции. Задачи создаются и назначаются устройствам с помощью мастера. Чтобы быстрее и проще назначить задачу устройствам, вы можете указывать в окне мастера устройства удобным для вас способом:

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

Проблемы с удаленной деинсталляцией

При удаленной деинсталляции приложений сторонних производителей, администраторы могут столкнуться с предупреждением: "Удаление на этом устройстве завершено с предупреждениями: Приложение для деинсталляции не установлено". Эта проблема обычно возникает, когда приложение, которое нужно удалить, установлено только для текущего пользователя, вошедшего в систему. Если пользователь не вошел в систему, такое приложение становится невидимым и его удаленная деинсталляция невозможна.

Такое поведение отличается от поведения приложений, предназначенных для использования несколькими пользователями на одном устройстве, когда приложения видны и доступны всем пользователям устройства.

В Kaspersky Security Center алгоритм регистрации приложений обрабатывает приложения для отдельных пользователей и приложения для нескольких пользователей по-разному:

- Приложения для нескольких пользователей поддерживаются в актуальном состоянии в реальном времени в списке установленных приложений.
- Приложения для отдельных пользователей отслеживаются с использованием механизма кеширования.

  Если в момент обнаружения приложения пользователь был в системе, Kaspersky Security Center кеширует информацию о приложениях этого пользователя. Даже если пользователь затем выходит из системы, на основе закешированных данных Kaspersky Security Center продолжает отображать эти приложения как установленные, хотя они больше не видны или доступны на устройстве.

Это несоответствие может привести к ситуациям, когда на основе закешированных данных Kaspersky Security Center определяет приложение как установленное, но задача удаления приложения не выполняется, потому что приложение становится недоступно, когда пользователь выходит из системы.

По умолчанию срок хранения кешированных данных приложения равен 30 дней. Администраторы могут изменить этот параметр, чтобы сократить время хранения данных в кеше с целью минимизировать расхождения между отображаемыми данными и реальной видимостью приложения на устройствах.

Чтобы настроить время хранения данных в кеше на один час (3600 секунд), выполните следующую команду на Сервере администрирования:

```
klscflag -fset -pv klserver -n KLNAG_INV_PERUSER_APPS_CACHE_NONACTIVE_SIDS_LIFETIME_SEC
-t d -v 3600
```

После выполнения этой команды перезагрузите Сервер администрирования, чтобы изменения вступили в силу.

Источники информации об установленных приложениях

Агент администрирования получает информацию о программном обеспечении, установленном на устройствах Windows, из следующих ключей реестра:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о приложениях, установленных для всех пользователей.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о приложениях, установленных для всех пользователей.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о приложениях, установленных для текущего пользователя.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о приложениях, установленных для набора пользователей.

Удаленная деинсталляция приложения с клиентских устройств группы администрирования

Чтобы удаленно деинсталлировать приложение с клиентских устройств группы администрирования:

1. Подключитесь к Серверу администрирования, под управлением которого находится нужная группа администрирования.

2. В дереве консоли выберите группу администрирования.

3. В рабочей области выберите вкладку **Задачи**.

4. Запустите мастер создания задачи по кнопке **Новая задача**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

В окне **Выбор типа задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** в папке **Дополнительно** выберите тип задачи **Удаленная деинсталляция приложения**.

В результате работы мастера создания задачи будет создана групповая задача удаленной деинсталляции выбранного приложения. Созданная задача отображается в рабочей области группы администрирования, на вкладке **Задачи**.

5. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной деинсталляции выбранное приложение будет удалено с клиентских устройств группы администрирования.

Удаленная деинсталляция приложения с выбранных устройств

Чтобы удаленно деинсталлировать приложение с выбранных устройств:

1. В дереве консоли выберите папку **Задачи**.

2. Запустите процесс создания задачи по кнопке **Новая задача**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

   В окне **Выбор типа задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** в папке **Дополнительно** выберите тип задачи **Удаленная деинсталляция приложения**.

   В результате работы мастера создания задачи будет создана задача удаленной деинсталляции выбранного приложения для выбранного набора устройств. Созданная задача отображается в рабочей области папки **Задачи**.

3. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранное приложение будет удалено с выбранных устройств.

Работа с инсталляционными пакетами

При создании задач удаленной установки используются инсталляционные пакеты, которые содержат набор параметров, необходимых для установки приложения.

> Инсталляционные пакеты могут содержать в себе файл ключа. Не рекомендуется размещать в открытом доступе инсталляционные пакеты, содержащие в себе файл ключа.

Вы можете использовать один и тот же инсталляционный пакет многократно.

Сформированные Сервером администрирования инсталляционные пакеты размещаются в дереве консоли в папке **Удаленная установка** во вложенной папке **Инсталляционные пакеты**. На Сервере администрирования инсталляционные пакеты хранятся в заданной папке общего доступа в служебной папке Packages.

При необходимости вы можете удалить инсталляционный пакет из вложенной папки **Инсталляционные пакеты**, следуя инструкциям в статье Удаление объекта.

Не меняйте вручную содержимое инсталляционных пакетов в общей папке. При необходимости вы можете создать копию инсталляционного пакета, внести необходимые изменения и создать задачи установки.

Создание инсталляционного пакета.

В этом разделе описана процедура создания следующих типов инсталляционных пакетов:

- инсталляционный пакет приложения "Лаборатории Касперского";
- инсталляционный пакет указанного исполняемого файла";
- инсталляционный пакет приложения из базы "Лаборатории Касперского".

Инсталляционный пакет для удаленной установки Агента администрирования не нужно создавать вручную. Он формируется автоматически при установке приложения Kaspersky Security Center и располагается в папке **Инсталляционные пакеты**. Если пакет для удаленной установки Агента администрирования был удален, то для его повторного формирования в качестве файла с описанием вам нужно выбрать файл nagent.kud, расположенный в папке NetAgent дистрибутива Kaspersky Security Center.

Чтобы создать инсталляционный пакет:

1. Подключитесь к нужному Серверу администрирования.
2. В дереве консоли выберите папку **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.
3. Запустите процесс создания автономного инсталляционного пакета одним из следующих способов:
   - В контекстном меню папки **Инсталляционные пакеты** выберите пункт **Новый** → **Инсталляционный пакет**.
   - В контекстном меню пустого списка инсталляционных пакетов выберите пункт **Новый** → **Инсталляционный пакет**.
   - Перейдите по ссылке **Создать инсталляционный пакет** в блоке управления списком инсталляционных пакетов.

   Запустится мастер создания инсталляционного пакета.
4. Выберите один из следующих типов инсталляционных пакетов, нажав на соответствующий значок:
   - Инсталляционный пакет приложения "Лаборатории Касперского".
   - Инсталляционный пакет указанного исполняемого файла.
   - Инсталляционный пакет приложения из базы "Лаборатории Касперского".

5. Укажите имя инсталляционного пакета, который будет создан.

   Вы можете указать любое имя.

6. Выберите приложение или исполняемый файл, для которого требуется создать инсталляционный пакет, одним из следующих способов:

   - Нажмите на кнопку **Обзор** и в стандартном окне **Открыть** выберите дистрибутив нужного приложения, расположенный на доступных дисках.

     Этот вариант применим, если вы выбрали создание инсталляционного пакета для приложения "Лаборатории Касперского" или для указанного исполняемого файла.

   - Нажмите на кнопку **Обзор** и в окне **Выбор приложения** выберите дистрибутив нужного приложения.

     Этот вариант применим, если вы выбрали создание инсталляционного пакета для приложений из базы "Лаборатории Касперского".

   Если вы создаете инсталляционный пакет для Сервера администрирования, выберите файл sc.kud. Файл sc.kud находится в корневой папке дистрибутива Kaspersky Security Center.

   Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.

7. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности.

   При создании инсталляционного пакета приложения вам может быть предложено просмотреть и принять Лицензионное соглашение и Политику конфиденциальности этого приложения.

   Прочтите оба документа. Если вы согласны со всеми условиями Лицензионного соглашения и Политики конфиденциальности, примите их, установив соответствующие флажки.

   Установка приложения на ваше устройство продолжится, и создание инсталляционного пакета возобновится.

   Если вы создаете инсталляционный пакет приложения Kaspersky Endpoint Security для Mac, вы можете выбрать язык Лицензионного соглашения и Политики конфиденциальности.

8. При необходимости включите автоматическую установку компонентов системы.

   Если вы создаете инсталляционный пакет приложения из базы "Лаборатории Касперского", вы можете включить автоматическую установку необходимых системных компонентов. Мастер создания инсталляционного пакета отображает список всех возможных общесистемных компонентов для выбранного приложения. Вы можете получить доступ к этому списку в свойствах инсталляционного пакета в любое время.

   Если вы создаете инсталляционный пакет патча, в список будут включены все системные компоненты, необходимые для развертывания этого патча.

9. Нажмите на кнопку **Готово**, чтобы завершить создание пакета.

После завершения работы мастера созданный инсталляционный пакет отобразится в рабочей области папки **Инсталляционные пакеты**.

Создание автономного инсталляционного пакета

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

Автономный инсталляционный пакет представляет собой исполняемый файл (installer.exe), который можно разместить на Веб-сервере, в общей папке или передать на клиентское устройство другим способом. Можно также отправить ссылку на автономный инсталляционный пакет по электронной почте. Полученный файл можно запустить локально на клиентском устройстве для выполнения установки приложения без участия Kaspersky Security Center.

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

Вы можете создавать автономные инсталляционные пакеты как для приложений "Лаборатории Касперского", так и для приложений сторонних производителей для Windows, macOS и Linux. Чтобы создать автономный инсталляционный пакет для приложений сторонних производителей, необходимо сначала создать пользовательский инсталляционный пакет.

Источником для создания автономных инсталляционных пакетов являются инсталляционные пакеты в списке созданных на Сервере администрирования.

Чтобы создать автономный инсталляционный пакет:

1. В дереве консоли выберите узел **Сервер администрирования → Дополнительно → Удаленная установка → Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. В списке инсталляционных пакетов выберите инсталляционный пакет, для которого требуется создать автономный пакет.

3. В контекстном меню выберите пункт **Создать автономный инсталляционный пакет**.

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

4. На первой странице мастера, если вы выбрали инсталляционный пакет для приложения "Лаборатории Касперского" и хотите установить Агент администрирования вместе с выбранным приложением, убедитесь, что параметр **Установить Агент администрирования совместно с данным приложением** включен.

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

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

Если автономный инсталляционный пакет для выбранного приложения уже существует на Сервере администрирования, мастер отобразит сообщение об этом. В этом случае вам нужно выбрать одно из следующих действий:

- **Создать автономный инсталляционный пакет**. Выберите этот параметр, например, если вы хотите создать автономный инсталляционный пакет для новой версии приложения, и чтобы также остался автономный инсталляционный пакет для предыдущей версии приложения, который вы создали ранее. Новый автономный инсталляционный пакет расположен в другой папке.

- **Использовать существующий автономный инсталляционный пакет**. Выберите этот параметр, если вы хотите использовать существующий автономный инсталляционный пакет. Процесс создания пакета не запускается.

- **Сформировать заново существующий автономный инсталляционный пакет**. Выберите этот параметр, если хотите создать автономный инсталляционный пакет для этого же приложения еще раз. Автономный инсталляционный пакет размещается в той же папке.

5. На следующей странице мастера выберите параметр **Переместить нераспределенные устройства в эту группу** и укажите группу администрирования, в которую вы хотите переместить клиентские устройства, после установки на них Агента администрирования.

   По умолчанию устройства перемещаются в группу **Управляемые устройства**.

   Если вы не хотите перемещать клиентское устройство в какую-либо группу администрирования после установки Агента администрирования, выберите параметр **Не перемещать устройства**.

6. На следующей странице мастера, после завершения процесса создания автономного инсталляционного пакета, отобразится результат создания автономного инсталляционного пакета и путь к нему.

   Можно перейти по ссылкам и выполнить следующие действия:

   - Открыть папку с автономным инсталляционным пакетом.

   - Отправить по электронной почте ссылку на созданный автономный инсталляционный пакет. Для этого необходимо, чтобы было запущено приложение для работы с электронной почтой.

   - Скопировать образец HTML-кода, чтобы разместить ссылку на веб-сайте. Текстовый файл (в формате TXT) создается и открывается с помощью приложения, связанного с TXT-форматом. В файле отображается HTML-тег <a> с атрибутами.

7. Если вы хотите открыть список автономных инсталляционных пакетов, на следующей странице мастера включите параметр **Открыть список автономных пакетов**.

8. Нажмите на кнопку **Готово**.

   Мастер создания автономного инсталляционного пакета закрывается.

Автономный инсталляционный пакет создан и помещен во вложенную папку Pkglnst общей папки Сервера администрирования. Вы можете просмотреть список автономных инсталляционных пакетов, нажав на кнопку **Просмотреть список автономных пакетов**, расположенную над списком инсталляционных пакетов.

Создание пользовательского инсталляционного пакета

Вы можете использовать пользовательские инсталляционные пакеты, чтобы:

- установить любое приложение (например, текстовый редактор) на клиентские устройства, например, с помощью задачи;
- создать автономный инсталляционный пакет.

Пользовательский инсталляционный пакет – это папка с набором файлов. Источником для создания пользовательского инсталляционного пакета является *архивный файл*. Архивный файл содержит файл или файлы, которые должны быть включены в пользовательский инсталляционный пакет. Создавая пользовательский инсталляционный пакет, вы можете указать параметры командной строки, например, для установки приложения в тихом режиме.

Чтобы создать пользовательский инсталляционный пакет:

1. В дереве консоли выберите **Сервер администрирования** → **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. Нажмите на кнопку **Создать инсталляционный пакет** над списком инсталляционных пакетов.

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

3. На первой странице мастера выберите параметр **Создать инсталляционный пакет для указанного исполняемого файла**.

4. На следующей странице мастера укажите имя пользовательского инсталляционного пакета.

5. На следующей странице мастера нажмите на кнопку **Обзор** и в стандартном окне **Открыть** выберите файл архива, расположенный на доступных дисках, чтобы создать пользовательский инсталляционный пакет.

   Вы можете загрузить архивный файл формата ZIP, CAB, TAR или TAR.GZ. Создать инсталляционный пакет из файла формата SFX (самораспаковывающийся архив) невозможно.

   Файлы загружены на Сервер администрирования Kaspersky Security Center.

6. На следующей странице мастера укажите параметры командной строки для исполняемого файла.

   Вы можете указать параметры командной строки для установки приложения из инсталляционного пакета в тихом режиме. Указывать параметры командной строки необязательно.

   При необходимости настройте следующие параметры:

   - **Копировать всю папку в инсталляционный пакет**

     Выберите этот параметр, если исполняемый файл сопровождается дополнительными файлами, необходимыми для установки приложения. Прежде чем включить этот параметр, убедитесь, что все требуемые файлы хранятся в одной папке. Если этот параметр включен, приложение добавляет все содержимое папки, включая указанный исполняемый файл, в инсталляционный пакет.

   - **Конвертировать параметры на рекомендуемые значения для приложений, распознаваемых Kaspersky Security Center**

     Приложение будет установлено с рекомендуемыми параметрами, если информация об указанном приложении содержится в базе данных "Лаборатории Касперского".

     Если вы ввели параметры в поле **Параметры запуска исполняемого файла**, они будут изменены на рекомендуемые параметры.

По умолчанию параметр включен.

База данных "Лаборатории Касперского" создана и поддерживается аналитиками "Лаборатории Касперского". Для каждого приложения, добавляемого в базу данных, аналитики "Лаборатории Касперского" определяют оптимальные параметры установки. Параметры определяются так, чтобы обеспечить успешную удаленную установку приложения на клиентское устройство. База данных обновляется автоматически при запуске задачи Загрузка обновлений в хранилище Сервера администрирования.

Начнется процесс создания пользовательского инсталляционного пакета.

В окне мастера отобразится информация о завершении процесса.

Если пользовательский инсталляционный пакет не создан, отобразится соответствующее сообщение.

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

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

В списке инсталляционных пакетов на Сервере администрирования можно просмотреть и изменить свойства пользовательского инсталляционного пакета.

Просмотр и изменение свойств пользовательских инсталляционных пакетов

После создания пользовательского инсталляционного пакета в окне свойств можно просмотреть общую информацию о нем и указать параметры установки.

Чтобы просмотреть и изменить свойства пользовательского инсталляционного пакета:

1. В дереве консоли выберите **Сервер администрирования** → **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

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

   Откроется окно свойств выбранного инсталляционного пакета.

3. Отобразится следующая информация:

   - название инсталляционного пакета;
   - название приложения, упакованного в пользовательский инсталляционные пакет;
   - версия приложения;
   - дата создания инсталляционного пакета;
   - путь к пользовательскому инсталляционному пакету на Сервере администрирования;
   - параметры запуска исполняемого файла.

4. Задайте следующие параметры:

   - Название инсталляционного пакета
   - **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.

     > Этот параметр доступен, только если приложение, добавленное в инсталляционный пакет, было распознано Kaspersky Security Center.

   - **Параметры запуска исполняемого файла**

     Если приложению требуются дополнительные параметры для установки без вывода сообщений, укажите их в этом поле. Дополнительную информацию см. в документации производителя.

     Вы также можете указать и другие параметры.

     > Эта параметр доступен только для пакетов, которые не были созданы на основе приложений "Лаборатории Касперского".

5. Нажмите на кнопку **OK** или **Применить**, чтобы сохранить изменения.

Новые параметры сохранены.

Получение инсталляционного пакета Агента администрирования из комплекта поставки Kaspersky Security Center

Вы можете получить инсталляционный пакет Агента администрирования из комплекта поставки Kaspersky Security Center без необходимости установки Kaspersky Security Center. Затем вы можете использовать инсталляционный пакет для установки Агента администрирования на клиентские устройства.

Чтобы получить инсталляционный пакет Агента администрирования из комплекта поставки Kaspersky Security Center:

1. Запустите исполняемый файл ksc_<номер версии>.<номер сборки>_full_<язык локализации>.exe из дистрибутива Kaspersky Security Center.
2. В появившемся окне перейдите по ссылке **Извлечь инсталляционные пакеты**.
3. В списке инсталляционных пакетов установите флажок рядом с инсталляционным пакетом Агента администрирования и нажмите на кнопку **Далее**.
4. При необходимости нажмите на кнопку **Обзор**, чтобы изменить отображаемую папку для извлечения инсталляционного пакета.

5. Нажмите на кнопку **Распаковать**.

   Приложение извлекает инсталляционный пакет Агента администрирования.

6. После завершения процесса, нажмите на кнопку **Закрыть**.

Инсталляционный пакет Агента администрирования распаковывается в выбранную папку.

С помощью инсталляционного пакета вы можете установить Агент администрирования одним из следующих способов:

- Локально запустив файл setup.exe из извлеченной папки.
- С помощью автоматической установки.
- С помощью механизма групповых политик Microsoft Windows.

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 **Выбор типа задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** в папке **Дополнительно** выберите тип задачи **Распространение инсталляционного пакета**.

   В результате работы мастера создания задачи будет создана задача распространения выбранных инсталляционных пакетов на выбранные подчиненные Серверы администрирования.
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.

Распространение инсталляционных пакетов с помощью точек распространения

Для распространения инсталляционных пакетов в пределах группы администрирования вы можете использовать точки распространения.

После получения инсталляционных пакетов с Сервера администрирования точки распространения автоматически распространяют их на клиентские устройства с помощью многоадресной IP-рассылки. IP-рассылка новых инсталляционных пакетов в пределах группы администрирования производится один раз. Если в момент рассылки клиентское устройство было отключено от сети организации, то при запуске задачи установки Агент администрирования клиентского устройства автоматически скачивает необходимый инсталляционный пакет с точки распространения.

Передача в Kaspersky Security Center информации о результатах установки приложения

После создания инсталляционного пакета приложения вы можете настроить инсталляционный пакет таким образом, чтобы диагностическая информация о результатах установки приложения передавалась в Kaspersky Security Center. Для инсталляционных пакетов приложений "Лаборатории Касперского" передача диагностической информации о результате установки приложений настроена по умолчанию, дополнительная настройка не требуется.

Чтобы настроить передачу в Kaspersky Security Center диагностической информации о результате установки приложения:

1. Перейдите в папку инсталляционного пакета, сформированного средствами Kaspersky Security Center для выбранного приложения. Эта папка расположена в папке общего доступа, которая была указана при установке Kaspersky Security Center.

2. Откройте файл с расширением kpd или kud для редактирования (например, с помощью текстового редактора "Блокнот" Microsoft Windows).

   Файл имеет формат обычного конфигурационного ini-файла.

3. Добавьте в файл следующие строки:

   ```
   [SetupProcessResult]
   Wait=1
   ```

   Эта команда настраивает приложение Kaspersky Security Center таким образом, чтобы оно ожидало окончания установки приложения, для которого сформирован инсталляционный пакет, и анализировало код возврата программы установки. Если нужно отключить передачу диагностической информации, установите для ключа Wait значение 0.

4. Внесите описание кодов возврата успешной установки. Для этого добавьте в файл следующие строки:

   ```
   [SetupProcessResult_SuccessCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   ...
   ```

   В квадратных скобках приводятся необязательные ключи.

   Синтаксис строк:

   - `<return code>`. Любое число, соответствующее коду возврата приложения установки. Количество кодов возврата может быть произвольным.

   - `<description>`. Текстовое описание результата установки. Описание может отсутствовать.

5. Внесите описание кодов возврата для установки, завершенной с ошибкой. Для этого добавьте в файл следующие строки:

   ```
   [SetupProcessResult_ErrorCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   ...
   ```

   Синтаксис строк соответствует синтаксису строк кодов возврата при успешной установке.

6. Закройте kpd- или kud-файл, сохранив внесенные изменения.

Информация о результатах установки приложения, указанного пользователем, будет записываться в журнал Kaspersky Security Center и отображаться в списке событий, в отчетах и в результатах выполнения задач.

Определение адреса прокси-сервера KSN для инсталляционных пакетов

В случае изменения адреса или домена Сервера администрирования вы можете указать адрес прокси-сервера KSN для инсталляционного пакета.

Чтобы определить адрес прокси-сервера KSN для инсталляционного пакета:

1. В дереве консоли в папке **Удаленная установка** двойным щелчком мыши нажмите на вложенную папку **Инсталляционные пакеты**.
2. В появившемся окне нажмите на кнопку **Свойства**.
3. В отобразившемся окне свойств выберите подраздел **Общие**.
4. В подразделе **Общие** окна свойств введите адрес прокси-сервера KSN.

Инсталляционные пакеты будут использовать этот адрес по умолчанию.

Получение актуальных версий приложений

Kaspersky Security Center позволяет получать актуальные версии корпоративных приложений, хранящиеся на серверах "Лаборатории Касперского".

Чтобы получить актуальные версии корпоративных приложений "Лаборатории Касперского":

1. Выполните одно из следующих действий:

   - В дереве консоли выберите узел с именем нужного вам Сервера администрирования на вкладке **Мониторинг** в разделе **Развертывание** перейдите по ссылке **Вышли новые версии приложений "Лаборатории Касперского"**.

     Ссылка **Вышли новые версии приложений "Лаборатории Касперского"** становится доступна, когда Сервер администрирования обнаруживает очередную версию корпоративного приложения на интернет-сервере "Лаборатории Касперского".

   - В дереве консоли выберите **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**, в рабочей области нажмите **Дополнительные действия** и в раскрывающемся списке выберите пункт **Просмотреть актуальные версии приложений "Лаборатории Касперского"**.

   Появится список текущих версий приложений "Лаборатории Касперского".

2. Можно отфильтровать список приложений "Лаборатории Касперского", чтобы упростить поиск нужного приложения.

   В верхней части окна **Текущие версии приложений** перейдите по ссылке **Фильтр** для фильтрации списка приложений по следующим критериям:

   - **Компоненты**. Используйте этот критерий, чтобы отфильтровать список приложений "Лаборатории Касперского" по областям защиты, которые используются в вашей сети.
   - **Тип ПО для загрузки**. Используйте этот критерий, чтобы отфильтровать список приложений "Лаборатории Касперского" по типу приложения.
   - **Какие обновления и ПО показывать**. Используйте этот критерий, чтобы отобразить доступные приложения "Лаборатории Касперского" по определенным версиям.
   - **На каких языках показывать ПО и обновления**. Используйте этот критерий для отображения приложений "Лаборатории Касперского" с определенным языком локализации.

   Нажмите на кнопку **Применить**, чтобы применить изменения.

3. Выберите в списке нужное вам приложение.

4. Загрузите дистрибутив приложения по ссылке в строке **Веб-адрес дистрибутива**.

   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.

Если для выбранного приложения отображается кнопка **Загрузить приложения и создать инсталляционные пакеты**, вы можете нажать на эту кнопку для загрузки дистрибутива приложения и автоматического создания инсталляционного пакета. Kaspersky Security Center загружает дистрибутив приложения на Сервер администрирования в папку общего доступа, заданную при установке Kaspersky Security Center. Список автоматически созданных инсталляционных пакетов отображается в папке дерева консоли **Удаленная установка**, во вложенной папке **Инсталляционные пакеты**.

После закрытия окна **Текущие версии приложений** ссылка **Вышли новые версии приложений "Лаборатории Касперского"** исчезнет из раздела **Развертывание**.

Вы можете создавать инсталляционные пакеты новых версий приложений и работать с созданными инсталляционными пакетами в папке **Удаленная установка** дерева консоли, во вложенной папке **Инсталляционные пакеты**.

Вы также можете открыть окно **Текущие версии приложений** по ссылке **Просмотреть актуальные версии приложений "Лаборатории Касперского"** в рабочей области папки **Инсталляционные пакеты**.

Подготовка устройства под управлением Windows к удаленной установке

Удаленная установка программы на клиентском устройстве может завершаться с ошибкой по следующим причинам:

- Задача ранее уже была успешно выполнена на этом устройстве.

  В этом случае ее повторное выполнение не требуется.

- Во время запуска задачи устройство было выключено.

  В этом случае требуется включить устройство и запустить задачу еще раз.

- Отсутствует связь между Сервером администрирования и Агентом администрирования, установленным на клиентском устройстве.

  Для определения причины проблемы вы можете воспользоваться утилитой удаленной диагностики клиентского устройства (klactgui).

- Если на устройстве не установлен Агент администрирования, при удаленной установке приложения могут возникнуть следующие ситуации:

  - на клиентском устройстве включен **Отключить простой общий доступ к файлам**;
  - на клиентском устройстве не работает служба Server;
  - на клиентском устройстве закрыты необходимые порты;
  - у учетной записи, под которой выполняется задача, недостаточно прав.

Для того чтобы избежать проблем, которые могут возникнуть при установке приложения на клиентское устройство без установленного Агента администрирования, необходимо действовать, как описано в разделе принудительного развертывания с помощью задачи удаленной установки Kaspersky Security Center.

Ранее использовалась утилита riprep для подготовки устройства к удаленной установке. Теперь это считается устаревшим способом настройки операционных систем. Утилиту riprep не рекомендуется использовать на операционных системах выше Windows XP и Windows Server 2003 R2.

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".
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`.

b. 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.

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

d. 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`

e. Сохраните и закройте файл sudoers.

f. Повторно подключитесь к устройству через SSH и проверьте, что служба sudo не требует пароль, с помощью команды `sudo whoami`.

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`.

Подготовка устройства под управлением SUSE Linux Enterprise Server 15 к установке Агента администрирования

Чтобы установить Агент администрирования на устройство с операционной системой SUSE Linux Enterprise Server 15,

перед установкой Агента администрирования выполните следующую команду:

```
sudo zypper install insserv-compat
```

Это позволит вам установить пакет insserv-compat и правильно настроить Агент администрирования.

Выполните команду `rpm -q insserv-compat`, чтобы проверить, если пакет уже установлен.

Если в вашей сети много устройств под управлением SUSE Linux Enterprise Server 15, вы можете использовать специальное программное обеспечение для настройки и управления инфраструктурой компании. Используя это программное обеспечение, вы можете автоматически установить пакет insserv-compat сразу на все необходимые устройства. Например, вы можете использовать Puppet, Ansible, Chef, или сделать свой скрипт любым удобным для вас способом.

Если на устройстве нет ключей подписи GPG для SUSE Linux Enterprise, вы можете увидеть следующее предупреждение: `Package header is not signed!` Выберите параметр `i`, чтобы игнорировать предупреждение.

Помимо установки пакета insserv-compat, убедитесь, что ваши Linux-устройства полностью подготовлены. После этого разверните и установите Агент администрирования.

Подготовка устройства с операционной системой macOS к удаленной установке Агента администрирования

Чтобы подготовить устройство с операционной системой macOS к удаленной установке Агента администрирования:

1. Убедитесь, что на целевом устройстве с операционной системой macOS установлено приложение sudo.

2. Выполните проверку конфигурации устройства:

   a. Убедитесь, что порт 22 открыт на клиентском устройстве. Для этого в разделе **Системные настройки** откройте панель **Обмен** и убедитесь, что установлен флажок **Удаленный вход**.

   Вы можете подключиться к клиентскому устройству по протоколу Secure Shell (SSH) только через порт 22. Вы не можете изменить номер порта.

   Вы можете использовать команду `ssh <имя_устройства>` для удаленного входа на устройство macOS. В панели **Общий доступ** можно использовать параметр **Разрешить доступ для** чтобы задать область действия пользователей, которым разрешен доступ к устройству macOS.

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

   Используйте команду `sudo visudo`, чтобы открыть конфигурационный файл sudoers в терминале. В файле, который вы открыли, в поле `Спецификация привилегий пользователя` укажите следующее: `username ALL = (ALL) NOPASSWD: ALL`. В этом случае `username` является учетной записью пользователя, которая будет использоваться для подключения к устройству по протоколу SSH.

   c. Сохраните и закройте файл sudoers.

   d. Повторно подключитесь к устройству через SSH и проверьте, что служба sudo не требует пароль, с помощью команды `sudo whoami`.

3. Загрузите и создайте инсталляционный пакет:

   a. Загрузите инсталляционный пакет Агента администрирования одним из следующих способов:

      - В дереве консоли, в контекстном меню выбрав **Удаленная установка** → **Инсталляционные пакеты** и далее **Показать текущие версии приложений**, чтобы выбрать из доступных пакетов.
      - Загрузив соответствующую версию Агента администрирования с веб-сайта Службы технической поддержки по адресу https://support.kaspersky.ru/.
      - Запросив инсталляционный пакет у специалистов Службы технической поддержки.

   b. Для создания пакета удаленной установки используйте файлы:

      - klnagent.kud
      - install.sh
      - klnagentmac.dmg

4. Создайте задачу удаленной установки приложения с параметрами:

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

Клиентское устройство готово к удаленной установке Агента администрирования с помощью соответствующей задачи, которую вы создали.

Приложения "Лаборатории Касперского": лицензирование и активация

В этом разделе описаны возможности Kaspersky Security Center по работе с лицензионными ключами управляемых приложений "Лаборатории Касперского".

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

При добавлении лицензионного ключа с помощью Kaspersky Security Center свойства лицензионного ключа сохраняются на Сервере администрирования. На основании этой информации приложение формирует отчет об использовании лицензионных ключей и уведомляет администратора об истечении сроков действия лицензий и о превышении лицензионных ограничений, заложенных в свойствах лицензионных ключей. Вы можете настраивать параметры оповещений об использовании лицензионных ключей в составе параметров Сервера администрирования.

Лицензирование управляемых приложений

Приложения "Лаборатории Касперского" установленные на управляемых устройствах, должны быть активированы путем применения файла ключа или кода активации к каждому из приложений. Файл ключа или код активации может быть распространен следующими способами:

- с помощью автоматического распространения;
- с помощью инсталляционного пакета управляемого приложения;
- с помощью задачи *Добавление лицензионного ключа* управляемого приложения;
- активация управляемого приложения вручную.

Вы можете добавить активный или резервный лицензионный ключ любым из перечисленных выше способов. Приложение "Лаборатории Касперского" использует активный в данный момент ключ и сохраняет резервный ключ, который будет применяться после истечения срока действия активного ключа. Приложение, для которого вы добавляете лицензионный ключ, определяет, является ли ключ активным или резервным. Определение ключа не зависит от способа, который вы используете для добавления лицензионного ключа.

Автоматическое распространение

> Если вы используете разные управляемые приложения и вам важно распространить определенный файл ключа или код активации на устройства, используйте другие способы распространения кода активации или файла ключа.

Kaspersky Security Center позволяет автоматически распространять имеющиеся лицензионные ключи на устройства. Например, в хранилище Сервера администрирования находится три лицензионных ключа. Для всех лицензионных ключей установлен флажок **Автоматически распространять лицензионный ключ на управляемые устройства**. На устройствах организации установлено приложение безопасности "Лаборатории Касперского", например, Kaspersky Endpoint Security для Windows. Обнаружено новое устройство, на которое необходимо распространить лицензионный ключ. Приложение определяет, что для этого устройства подходит, например, два лицензионных ключа из хранилища, лицензионный ключ *Ключ_1* и лицензионный ключ *Ключ_2*. На устройство распространяется один из подходящих лицензионных ключей. В этом случае невозможно предсказать, какой из этих двух лицензионных ключей будет распространен на данное устройство, так как автоматическое распространение лицензионных ключей не предполагает вмешательства администратора.

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

Перед распространением файл ключа или код активации необходимо добавить в хранилище Сервера администрирования.

Инструкции:

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

  Или

- Kaspersky Security Center Web Console:
  - Добавление лицензионного ключа в хранилище Сервера администрирования.
  - Автоматическое распространение лицензионного ключа.

Обратите внимание, что автоматически распространяемый лицензионный ключ может не отображаться в хранилище виртуального Сервера администрирования в следующих случаях:

- Лицензионный ключ недействителен для приложения.
- Виртуальный Сервер администрирования не имеет управляемых устройств.
- Лицензионный ключ уже используется для устройств, управляемых другим виртуальным Сервером администрирования, и достигнуто лицензионное ограничение на количество устройств.

Добавление файла ключа или кода активации в инсталляционный пакет управляемого приложения

Из соображений безопасности не рекомендуется использовать этот параметр. Файл ключа или код активации, добавленный в инсталляционный пакет, может быть скомпрометирован.

В случае установки управляемого приложения с помощью инсталляционного пакета вы можете указать код активации или файл ключа в инсталляционном пакете или в политике этого приложения. Лицензионный ключ распространится на управляемые устройства при очередной синхронизации устройства с Сервером администрирования.

Инструкции:

- Консоль администрирования:
  - Создание инсталляционного пакета.
  - Установка приложений на клиентские устройства.

  Или

- Kaspersky Security Center Web Console: Добавление лицензионного ключа в инсталляционный пакет.

Распространение с помощью задачи добавления лицензионного ключа управляемого приложения

В случае использования задачи *Добавление лицензионного ключа* управляемого приложения вы можете выбрать лицензионный ключ, который необходимо распространить на устройства, и выбрать устройства удобным вам способом, например, выбрав группу администрирования или выборку устройств.

Перед распространением файл ключа или код активации необходимо добавить в хранилище Сервера администрирования.

Инструкции:

- Консоль администрирования:
  - Добавление лицензионного ключа в хранилище Сервера администрирования.
  - Распространение лицензионного ключа на клиентские устройства.

  Или
- Kaspersky Security Center Web Console:
  - 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.

Просмотр информации об используемых лицензионных ключах

Чтобы просмотреть информацию об используемых лицензионных ключах,

В дереве консоли выберите папку **Лицензии "Лаборатории Касперского"**.

В рабочей области папки отображается перечень лицензионных ключей, используемых на клиентских устройствах.

Рядом с каждым лицензионным ключом отображается значок, соответствующий типу его использования:

-  – информация об используемом лицензионном ключе получена от подключенного к Серверу администрирования клиентского устройства. Файл этого лицензионного ключа не хранится на Сервере администрирования.
-  – лицензионный ключ находится в хранилище Сервера администрирования. Автоматическое распространение этого лицензионного ключа отключено.
-  – лицензионный ключ находится в хранилище Сервера администрирования. Включено автоматическое распространение этого лицензионного ключа.

Вы можете просмотреть информацию о том, какие лицензионные ключи используются для активации приложения на клиентском устройстве, в разделе **Приложения** окна свойств клиентского устройства.

Для определения актуальных параметров лицензионных ключей виртуального Сервера администрирования Сервер администрирования отправляет запрос на серверы активации "Лаборатории Касперского" не реже одного раза в сутки. Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы.

Если лицензионный ключ получен с клиентского устройства, вы не можете экспортировать его в виде файла.

Добавление лицензионного ключа в хранилище Сервера администрирования

Чтобы добавить лицензионный ключ в хранилище Сервера администрирования:

1. В дереве консоли выберите папку **Лицензии "Лаборатории Касперского"**.
2. Запустите задачу добавления лицензионного ключа одним из следующих способов:
   - В контекстном меню лицензионного ключа выберите пункт **Добавить код активации или файл ключа**.
   - Перейдите по ссылке **Добавить код активации или файл ключа** в блоке управления списком лицензионных ключей.
   - Нажмите на кнопку **Добавить код активации или файл ключа**.

   Запустится мастер Мастер добавления лицензионного ключа.
3. Выберите способ активации Сервера администрирования: с помощью кода активации или с помощью файла ключа.

4. Укажите ваш код активации или файл ключа.

5. Выберите параметр **Автоматически распространять лицензионный ключ на управляемые устройства**, если вы хотите распространить соответствующий лицензионный ключ в своей сети немедленно. Если вы не выберете этот параметр, вы можете позже вручную распространить лицензионный ключ.

В результате файл ключа загружается и Мастер добавления лицензионного ключа завершается. Теперь вы можете увидеть этот лицензионный ключ в списке лицензий "Лаборатории Касперского".

Удаление лицензионного ключа Сервера администрирования

Чтобы удалить лицензионный ключ Сервера администрирования:

1. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

2. В открывшемся окне свойств Сервера администрирования выберите раздел **Лицензионные ключи**.

3. Удалите лицензионный ключ, нажав на кнопку **Удалить**.

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.

Распространение лицензионного ключа на клиентские устройства

Kaspersky Security Center позволяет распространить лицензионный ключ на клиентские устройства с помощью задачи *Распространение лицензионного ключа*.

Перед распространением добавьте лицензионный ключ в хранилище Сервера администрирования.

Чтобы распространить лицензионный ключ на клиентские устройства:

1. В дереве консоли выберите папку **Лицензии "Лаборатории Касперского"**.

2. Нажмите на кнопку **Автоматически распространять лицензионный ключ на управляемые устройства** в блоке управления списком лицензионных ключей.

   Запустится мастер **Мастер создания задачи активации приложения**. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. В списке приложений выберите приложение, для которого вы хотите создать задачу.

4. На шаге мастера **Добавить ключ** добавьте лицензионный ключ, используя один из следующих параметров:

   - Выберите параметр **Код активации**, чтобы добавить код активации из хранилища Kaspersky Security Center.

     Нажмите на кнопку **Выбрать**. В открывшемся окне выберите код активации и нажмите на кнопку **OK**.

   - Выберите параметр **Файл ключа или ключ** и выполните следующие действия:

     a. Нажмите на кнопку **Выбрать**.

     b. В контекстном меню выберите один из пунктов:

     - **Файл ключа из папки**.

       В открывшемся окне выберите файл ключа на своем устройстве и нажмите на кнопку **Открыть**.

     - **Ключ из хранилища Kaspersky Security Center**.

       В открывшемся окне выберите ключ из хранилища Kaspersky Security Center и нажмите на кнопку **OK**.

5. Если вы хотите заменить активный лицензионный ключ, снимите флажок **Использовать ключ в качестве резервного**.

   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 ключ в качестве резервного**.

   Если вы хотите узнать больше о проблемах, которые могут возникнуть при добавлении лицензионного ключа в Kaspersky Security Center для Windows, и способах их решения, обратитесь к Базе знаний Kaspersky Security Center.

6. Проверьте информацию о лицензионном ключе и нажмите **Далее**.

7. На этом шаге мастера выберите устройства, которым вы хотите назначить задачу добавления ключа. Можно указать устройства (до 1000 устройств) одним из следующих способов:

   - **Выбрать устройства, обнаруженные в сети Сервером администрирования**. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

   - **Задать адреса устройств вручную или импортировать из списка**. Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

   - **Назначить задачу выборке устройств**. В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать предопределенную выборку или вашу собственную выборку.

   - **Назначить задачу группе администрирования**. В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.

8. На шаге **Настройка расписания запуска задачи** мастера можно составить расписание запуска задачи:

- **Запуск по расписанию**:
  - **Один раз**

    Задача выполняется один раз, в указанные дату и время (по умолчанию в день создания задачи).

  - **Вручную**

    Задача не запускается автоматически. Вы можете запустить задачу только вручную.

    По умолчанию выбран этот вариант.

  - **При загрузке обновлений в хранилище**

    Эта задача запускается после загрузки обновлений в хранилище. Например, вам может понадобиться это расписание для задачи поиска уязвимостей и требуемых обновлений.

  - **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 случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

9. На шаге мастера **Определение названия задачи** укажите название задачи. Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

10. На шаге **Завершение создания задачи** мастера нажмите на кнопку **Готово**, чтобы завершить работу мастера.

    Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

Задачи, сформированные при помощи мастера **Мастер создания задачи активации приложения**, являются задачами для наборов устройств и размещаются в папке **Задачи** дерева консоли.

Вы также можете создать групповую или локальную задачу распространения лицензионного ключа с помощью мастера создания задачи для группы администрирования и для клиентского устройства.

Автоматическое распространение лицензионного ключа

Kaspersky Security Center позволяет автоматически распространять на управляемые устройства лицензионные ключи, размещенные в хранилище ключей на Сервере администрирования. Автоматическое распространение лицензионных ключей не применяется к устройствам в папке **Нераспределенные устройства**.

Чтобы автоматически распространять лицензионный ключ на управляемые устройства:

1. В дереве консоли выберите папку **Лицензии "Лаборатории Касперского"**.
2. В рабочей области папки выберите лицензионный ключ, который вы хотите автоматически распространять на устройства.
3. Откройте окно свойств выбранного лицензионного ключа одним из следующих способов:
   - в контекстном меню лицензионного ключа выберите пункт **Свойства**;
   - по ссылке **Просмотреть свойства лицензионного ключа** в блоке работы с выбранным лицензионным ключом.
4. В открывшемся окне свойств лицензионного ключа установите флажок **Автоматически распространяемый лицензионный ключ**. Закройте окно свойств лицензионного ключа.

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.

Виртуальный Сервер администрирования автоматически распространяет лицензионные ключи из своего хранилища и из хранилища Сервера администрирования. Рекомендуется:

- Используйте задачу *Добавить лицензионный ключ*, чтобы выбрать лицензионный ключ, который необходимо развернуть на устройствах.
- Не выключайте параметр **Разрешить автоматическое распространение лицензионных ключей этого виртуального Сервера на его устройства** в параметрах виртуального Сервера администрирования. Иначе виртуальный Сервер администрирования не будет распространять лицензионные ключи на устройства, в том числе лицензионные ключи из хранилища Сервера администрирования.

Если вы установили флажок **Автоматически распространяемый лицензионный ключ** в окне свойств лицензионного ключа, лицензионный ключ будет немедленно распространен в вашей сети. Если вы не выберете этот параметр, вы можете позже вручную распространить лицензионный ключ.

Создание и просмотр отчета об использовании лицензионных ключей

Чтобы создать отчет об использовании лицензионных ключей на клиентских устройствах:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. Выберите шаблон отчета **Отчет об использовании лицензионных ключей** или создайте новый шаблон отчета одноименного типа.

В результате в рабочей области отчета об использовании лицензионных ключей отображается информация об активных и резервных лицензионных ключах, используемых на клиентских устройствах. Также в отчете содержатся сведения об устройствах, на которых используются лицензионные ключи, и об ограничениях, заданных в свойствах лицензионных ключей.

Просмотр информации о лицензионных ключах приложения

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

1. В дереве консоли Kaspersky Security Center выберите узел **Управляемые устройства** и перейдите на вкладку **Устройства**.
2. Откройте контекстное меню требуемого устройства по правой клавише мыши и выберите пункт **Свойства**.
3. В открывшемся окне свойств устройства выберите раздел **Приложения**.
4. В появившемся списке приложений выберите приложение, лицензионные ключи которого вы хотите просмотреть, и нажмите на кнопку **Свойства**.
5. В открывшемся окне свойств Сервера администрирования выберите раздел **Лицензионные ключи**.

   Информация отображается в рабочей области этого раздела.

Экспорт файла ключа

Если ваш лицензионный ключ был случайно удален и вы хотите его восстановить, вы можете экспортировать файл ключа с другого Сервера администрирования.

Чтобы экспортировать файл ключа, вам нужно иметь право **Экспорт файла ключа** в функциональной области **Общие функции: Управление лицензионными ключами**.

Если лицензионный ключ получен с клиентского устройства, вы не можете экспортировать его.

Чтобы экспортировать лицензионный ключ:

1. В дереве консоли выберите папку **Лицензии "Лаборатории Касперского"**.
2. В списке выберите ключ, который вы хотите экспортировать в виде файла.
3. В открывшемся информационном окне перейдите по ссылке **Экспортировать файл ключа**.
4. В открывшемся окне укажите путь к папке, в которой вы хотите сохранить файл ключа и укажите имя файла. Нажмите на кнопку **Сохранить**.

Файл лицензионного ключа с расширением .key будет экспортирован в выбранную папку.

Если лицензионный ключ, файл которого вы экспортировали, был добавлен в хранилище Сервера администрирования как код активации и вы хотите добавить экспортированный файл лицензионного ключа в хранилище другого Сервера администрирования, вам нужно ввести его как код активации, а не добавлять как файл ключа. Иначе возникнет ошибка. Вам необходимо открыть экспортированный файл лицензионного ключа в любом удобном текстовом редакторе и скопировать код активации.

Настройка защиты сети

В этом разделе содержится информация о настройке вручную политик и задач, о ролях пользователей, о построении структуры групп администрирования и об иерархии задач.

Сценарий: настройка защиты сети

Мастер первоначальной настройки создает политики и задачи с параметрами по умолчанию. Эти параметры могут оказаться не оптимальными или даже запрещенными в организации. Поэтому рекомендуется настроить эти политики и задачи и создать дополнительные политики и задачи, если это необходимо для вашей сети.

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- Установили Сервер администрирования Kaspersky Security Center.
- Установили Kaspersky Security Center Web Console (если требуется).
- Выполнили основной сценарий установки Kaspersky Security Center.

- Мастер первоначальной настройки завершен или следующие политики и задачи созданы вручную в группе администрирования **Управляемые устройства**:
  - политика Kaspersky Endpoint Security;
  - групповая задача обновления Kaspersky Endpoint Security;
  - политика Агента администрирования;
  - задача *Поиск уязвимостей и требуемых обновлений*.

Настройка защиты сети состоит из следующих этапов:

1. **Настройка и распространение политик и профилей политик для приложений "Лаборатории Касперского"**

   Для настройки и распространения параметров приложений "Лаборатории Касперского", установленных на управляемых устройствах, можно использовать два различных подхода управления безопасностью: ориентированный на пользователей и ориентированный на устройства. Можно комбинировать эти два подхода. Для реализации ориентированного на устройства метода управления безопасностью подходят средства Консоли администрирования на основе консоли управления Microsoft Management Console (MMC) и Kaspersky Security Center Web Console. Для реализации ориентированного на пользователей метода управления безопасностью подходит только Kaspersky Security Center Web Console.

2. **Настройка задач для удаленного управления приложениями "Лаборатории Касперского"**

   Проверьте задачи, созданные с помощью мастера первоначальной настройки, и при необходимости оптимизируйте их параметры.

   Инструкции:

   - Консоль администрирования:
     - Настройка групповой задачи обновления Kaspersky Endpoint Security.
     - Настройка расписания задачи Поиск уязвимостей и требуемых обновлений.
   - Kaspersky Security Center Web Console:
     - Настройка групповой задачи обновления Kaspersky Endpoint Security.
     - Параметры задачи поиска 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:

   - Консоль администрирования: Настройка максимального количества событий.
   - Kaspersky Security Center Web Console: Настройка максимального количества событий.

Результаты

После завершения этого сценария ваша сеть будет защищена благодаря настройке приложений "Лаборатории Касперского", задач и событий, получаемых Сервером администрирования:

- приложения "Лаборатории Касперского" настроены в соответствии с политиками и профилями политик.
- Управление приложениями осуществляется с помощью набора задач.
- Задано максимальное количество событий, которые могут храниться в базе данных.

После завершения настройки защиты сети вы можете приступить к настройке регулярных обновлений баз и приложений "Лаборатории Касперского".

Подробнее о настройке автоматического ответа на угрозы, обнаруженных Kaspersky Sandbox, см. в справке Kaspersky Sandbox 2.0.

Настройка и распространение политик: подход, ориентированный на устройства

После завершения этого сценария приложения будут настроены на всех управляемых устройствах в соответствии с политиками приложений и профилями политики, которые вы определяете.

Предварительные требования

Убедитесь, что вы установили Сервер администрирования Kaspersky Security Center и Kaspersky Security Center Web Console (если требуется). Если вы установили Kaspersky Security Center Web Console, вам может быть интересно также управление безопасностью, ориентированное на пользователей, в качестве альтернативы или дополнения к управлению безопасностью, ориентированному на устройства.

Этапы

Сценарий управления приложениями "Лаборатории Касперского", ориентированный на устройства, содержит следующие шаги:

1. **Настройка политик приложений**

   Настройте параметры установленных приложений "Лаборатории Касперского" на управляемых устройствах с помощью создания политики для каждого приложения. Этот набор политик будет применен к клиентским устройствам.

При настройке защиты сети с помощью мастера первоначальной настройки Kaspersky Security Center создает политику по умолчанию для следующих приложений:

- Kaspersky Endpoint Security для Windows – для клиентских устройств с операционной системой Windows.
- Kaspersky Endpoint Security для Linux – для клиентских устройств с операционной системой Linux.

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 Серверов администрирования и/или групп администрирования, подчиненные Серверы администрирования и дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами и подчиненными Серверами администрирования, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их выше по иерархии политики. Остальные незаблокированные параметры будут доступны для изменения в политике ниже по иерархии. Созданная иерархия политик позволяет эффективно управлять устройствами в группах администрирования.

Инструкции:

- Консоль администрирования: Создание политики.
- Kaspersky Security Center Web Console: 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:

- Консоль администрирования:
  - Создание профиля политики.
  - Создание правила активации профиля политики.
- Kaspersky Security Center Web Console:
  - Создание профиля политики.
  - Создание правила активации профиля политики.

3. **Распространение политик и профилей политик на управляемые устройства**

По умолчанию синхронизация управляемых устройств с Сервером администрирования происходит раз в 15 минут. Вы можете пропустить автоматическую синхронизацию и запустить синхронизацию вручную с помощью команды Синхронизировать принудительно. Также принудительная синхронизация выполняется после создания или изменения политики или профиля политики. Во время синхронизации новые или измененные политики и профили политик применяются к управляемым устройствам.

Если вы используете Kaspersky Security Center Web Console, можно проверить, доставлены ли политики и профили политик на устройства. Kaspersky Security Center определяет дату и время доставки в свойствах устройства.

Инструкции:

- Консоль администрирования: Принудительная синхронизация.
- Kaspersky Security Center Web Console: 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.

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. Для реализации ориентированного на устройства метода управления безопасностью подходят средства Консоли администрирования на основе консоли управления Microsoft Management Console (MMC) и Kaspersky Security Center Web Console. Для реализации ориентированного на пользователей метода управления безопасностью подходит только Kaspersky Security Center Web Console.

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.

Ручная настройка политики Kaspersky Endpoint Security

Этот раздел содержит рекомендации по настройке параметров политики Kaspersky Endpoint Security, которую создает мастер первоначальной настройки. Вы можете выполнить настройку в окне свойств политики.

При изменении параметра следует помнить, что для того, чтобы значение параметра использовалось на рабочей станции, следует нажать на кнопку с "замком" над параметром.

Настройка политики в разделе Продвинутая защита

Полное описание параметров этого раздела приведено в документации Kaspersky Endpoint Security для Windows.

В разделе **Продвинутая защита** можно настроить использование Kaspersky Security Network для Kaspersky Endpoint Security для Windows. Можно также настроить модули Kaspersky Endpoint Security для Windows, такие как Анализ поведения, Защита от эксплойтов, Предотвращение вторжений и Откат вредоносных действий.

В подразделе **Kaspersky Security Network** рекомендуется включить параметр **Kaspersky Security Network**. Использование этого параметра поможет перераспределить и оптимизировать трафик сети. Если параметр **Kaspersky Security Network** выключен, вы можете включить прямое использование серверов KSN.

Настройка политики в разделе Базовая защита

Полное описание параметров этого раздела приведено в документации Kaspersky Endpoint Security для Windows.

В разделе **Базовая защита** окна свойств политики рекомендуется указать дополнительные параметры в подразделах **Сетевой экран** и **Защита от файловых угроз**.

Подраздел **Сетевой экран** содержит параметры, позволяющие контролировать сетевую активность приложений на клиентских устройствах. Клиентское устройство использует сеть, которой присвоен один из следующих статусов: общедоступная, локальная или доверенная. В зависимости от состояния сети Kaspersky Endpoint Security может разрешить или запретить сетевую активность на устройстве. Когда вы добавляете новую сеть в свою организацию, вам нужно присвоить ей соответствующий сетевой статус. Например, если клиентским устройством является ноутбук, рекомендуется, чтобы это устройство использовало общедоступную или доверенную сеть, так как ноутбук не всегда подключен к локальной сети. В подразделе **Сетевой экран** можно проверить, правильно ли вы присвоили статусы используемым в вашей организации сетям.

Чтобы проверить список сетей:

1. В свойствах политики перейдите в раздел **Базовая защита** → **Сетевой экран**.
2. В блоке **Доступные сети** нажмите на кнопку **Настройки**.
3. В открывшемся окне **Сетевой экран** перейдите на вкладку **Сети** для просмотра списка сетей.

В подразделе **Защита от файловых угроз** можно отключить проверку сетевых дисков. Проверка сетевых дисков может создавать значительную нагрузку на сетевые диски. Целесообразнее осуществлять проверку непосредственно на файловых серверах.

Чтобы выключить проверку сетевых дисков:

1. В свойствах политики перейдите в раздел **Базовая защита** → **Защита от файловых угроз**.
2. В блоке **Уровень безопасности** нажмите на кнопку **Настройки**.
3. В открывшемся окне **Защита от файловых угроз** на вкладке **Общие** снимите флажок **Все сетевые диски**.

Настройка политики в разделе Дополнительные параметры

Полное описание параметров этого раздела приведено в документации Kaspersky Endpoint Security для Windows.

В разделе **Общие настройки** окна свойств политики, рекомендуется указать дополнительные параметры в подразделах **Отчеты и хранилище** и **Интерфейс**.

В подразделе **Отчеты и хранилище** перейдите в раздел **Передача данных на Сервер администрирования**. Флажок **О запускаемых приложениях** указывает, сохраняется ли в базе данных Сервера администрирования информация обо всех версиях всех модулей приложений на устройствах в сети организации. Если этот флажок установлен, сохраненная информация может занимать значительный объем в базе данных Kaspersky Security Center (десятки гигабайтов). Снимите флажок **О запускаемых приложениях**, если он установлен в политике верхнего уровня.

Если Консоль администрирования управляет защитой от угроз в сети организации централизованно, выключите отображение пользовательского интерфейса Kaspersky Endpoint Security для Windows на рабочих станциях. Для этого в подразделе **Интерфейс** перейдите в раздел **Взаимодействие с пользователем** и выберите параметр **Не отображать пользовательский интерфейс**.

Чтобы включить защиту паролем на рабочих станциях, в подразделе **Интерфейс** перейдите в раздел **Защита паролем**, нажмите на кнопку **Параметры** и установите флажок **Включить защиту паролем**.

Настройка политики в разделе Настройка событий

В разделе **Настройка событий** следует выключить сохранение на Сервере администрирования всех событий, за исключением перечисленных ниже:

- На вкладке **Критическое**:
  - *Автозапуск приложения выключен*
  - *Доступ запрещен*
  - *Запуск приложения запрещен*
  - *Лечение невозможно*
  - *Нарушено Лицензионное соглашение*
  - *Не удалось загрузить модуль шифрования*
  - *Невозможен запуск двух задач одновременно*
  - *Обнаружена активная угроза. Требуется запуск процедуры лечения активного заражения*
  - *Обнаружена сетевая атака*
  - *Обновлены не все компоненты*
  - *Ошибка активации*
  - *Ошибка активации портативного режима*
  - *Ошибка взаимодействия с Kaspersky Security Center*
  - *Ошибка деактивации портативного режима*
  - *Ошибка изменения состава компонентов приложения*
  - *Ошибка применения правил шифрования / расшифровки файлов*
  - *Политика не может быть применена*
  - *Процесс завершен*
  - *Сетевая активность запрещена*
- На вкладке **Отказ функционирования**: *Ошибка в настройках задачи. Настройки задачи не применены*

- На вкладке **Предупреждение**:
  - *Самозащита приложения выключена*
  - *Некорректный резервный ключ*
  - *Пользователь отказался от политики шифрования*
- На вкладке **Информационное сообщение**: *Запуск приложения запрещен в тестовом режиме.*

Ручная настройка групповой задачи обновления Kaspersky Endpoint Security

Оптимальный и рекомендуемый вариант расписания для Kaspersky Endpoint Security версии 10 и выше – **При загрузке обновлений в хранилище** при установленном флажке **Использовать автоматическое определение случайного интервала между запусками задачи**.

Ручная настройка групповой задачи проверки устройства Kaspersky Endpoint Security

Мастер первоначальной настройки создает групповую задачу проверки устройства. По умолчанию для задачи выбрано расписание **Запускать по пятницам в 19:00** с автоматической рандомизацией и снят флажок **Запускать пропущенные задачи**.

Это означает, что если устройства организации выключаются по пятницам, например, в 18:30, то задача проверки устройства никогда не будет запущена. Следует настроить оптимальное расписание этой задачи исходя из принятого в организации регламента работы.

Настройка расписания задачи Поиск уязвимостей и требуемых обновлений.

Мастер первоначальной настройки создает для Агента администрирования групповую задачу *Поиск уязвимостей и требуемых обновлений*. По умолчанию для задачи выбрано расписание **Запускать по вторникам в 19:00** с автоматической рандомизацией и установлен флажок **Запускать пропущенные задачи**.

Если регламент работы организации предусматривает выключение устройств в это время, то задача *Поиск уязвимостей и требуемых обновлений* будет запущена после включения устройства (в среду утром). Такое поведение может быть нежелательным, так как поиск уязвимостей может вызывать повышенную нагрузку на процессор и дисковую подсистему устройства. Следует настроить оптимальное расписание задачи исходя из принятого в организации регламента работы.

Ручная настройка групповой задачи установки обновлений и закрытия уязвимостей

Мастер первоначальной настройки создает для Агента администрирования групповую задачу установки обновлений и поиска уязвимостей. По умолчанию настроен запуск задачи ежедневно в 1:00 с автоматической рандомизацией, параметр **Запускать пропущенные задачи** выключен.

Если регламент работы организации предусматривает отключение устройств на ночь, то задача установки обновлений никогда не будет запущена. Следует задать оптимальное расписание задачи поиска уязвимостей исходя из принятого в организации регламента работы. Кроме того, следует учитывать, что в результате установки обновлений может потребоваться перезагрузка устройства.

Настройка количества событий в хранилище событий

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

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

Когда Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий Kaspersky Event Log. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления.

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

1. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

   Откроется окно свойств Сервера администрирования.

2. В разделе **Хранилище событий** укажите максимальное количество событий, хранящихся в базе данных.

3. Нажмите на кнопку **ОК**.

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.

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 контекстном меню Сервера администрирования выберите пункт **Свойства**.

   Откроется окно свойств Сервера администрирования.

2. В разделе **Хранилище событий** укажите максимальный срок хранения информации о закрытых уязвимостях в базе данных.

   Срок, заданный по умолчанию, – 90 дней.

3. Нажмите на кнопку **ОК**.

Максимальный срок хранения информации о закрытых уязвимостях ограничен указанным количеством дней. После этого задача обслуживания Сервера администрирования удалит устаревшую информацию из базы данных.

Управление задачами

Kaspersky Security Center управляет работой приложений, установленных на устройствах, путем создания и запуска различных задач. С помощью задач выполняются установка, запуск и остановка приложений, проверка файлов, обновление баз и модулей приложений, другие действия с приложениями.

Задачи делятся на следующие типы:

- *Групповые задачи*. Задачи, которые выполняются на устройствах выбранной группы администрирования.
- *Задачи Сервера администрирования*. Задачи, которые выполняются на Сервере администрирования.
- *Задачи для наборов устройств*. Глобальные задачи – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.
- *Локальные задачи*. Локальные задачи – это задачи, которые выполняются на конкретном устройстве.

Создание задач для приложения возможно только в случае, если на рабочее место администратора установлен плагин управления этим приложением.

Список устройств, для которых будет создана задача (до 1000 устройств), можно сформировать одним из следующих способов:

- Выбрать устройства, обнаруженные в сети Сервером администрирования.
- Задать список устройств вручную. 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 при подключении устройств или в результате обнаружения устройств.

Для каждого приложения вы можете создавать любое количество групповых задач, задач для наборов устройств и локальных задач.

Обмен информацией о задачах между приложением, установленным на устройстве, и информационной базой Kaspersky Security Center происходит в момент соединения Агента администрирования с Сервером администрирования.

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. При остановке приложения выполнение всех запущенных задач прекращается.

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

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

Управление задачами для приложений, поддерживающих мультитенантность

Групповая задача для мультитенантных приложений применяется к приложениям в зависимости от иерархии Серверов администрирования и клиентских устройств. Виртуальный Сервер администрирования, на котором создана задача, должен быть в той же группе администрирования, что и клиентское устройство, на котором установлено приложение, или в группе более низкого уровня.

В событиях, которые соответствуют результатам выполнения задачи, администратору поставщика услуг отображается информация об устройстве, на котором выполнена задача. В свою очередь, администратору тенанта отображается **Мультитенантный узел**.

Создание задачи

В Консоли администрирования можно создавать задачи непосредственно в папке группы администрирования, для которой создается задача, и в рабочей области папки **Задачи**.

Чтобы создать групповую задачу в папке группы администрирования:

1. В дереве консоли выберите группу администрирования, для которой нужно создать задачу.
2. В рабочей области выберите вкладку **Задачи**.
3. Запустите мастер создания задачи по кнопке **Создать задачу**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

*Чтобы создать задачу в рабочей области папки **Задачи**:*

1. В дереве консоли выберите папку **Задачи**.
2. Запустите мастер создания задачи по кнопке **Готово**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

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

Создание задачи Сервера администрирования

Сервер администрирования выполняет следующие функции:

- Рассылка отчетов.
- Загрузка обновлений в хранилище Сервера администрирования.
- Резервное копирование данных Сервера администрирования.
- Обслуживание Сервера администрирования.
- Выполнение синхронизации обновлений Центра обновления Windows.
- Создание инсталляционного пакета на основе образа ОС эталонного устройства.
- Удаленная установка приложений.
- Удаленная деинсталляция приложений.
- Распространять инсталляционные пакеты.
- Установка приложений на подчиненные Серверы администрирования.

На виртуальном Сервере администрирования доступна только задача автоматической рассылки отчетов и задача создания инсталляционного пакета на основе образа операционной системы эталонного устройства. В хранилище виртуального Сервера отображаются обновления, загруженные на главный Сервер администрирования. Резервное копирование данных виртуального Сервера осуществляется в рамках резервного копирования данных главного Сервера администрирования.

Чтобы создать задачу Сервера администрирования:

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания одним из следующих способов:
   - В контекстном меню папки дерева консоли **Задачи** выберите пункт **Создать → Задачу**.
   - В рабочей области папки **Создать задачу** нажмите на кнопку **Задачи**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

Задачи Загрузка обновлений в хранилище Сервера администрирования, Синхронизация обновлений Windows Update, Обслуживание Сервера администрирования и *Резервное копирование данных Сервера администрирования* можно создать только в одном экземпляре. Если задачи *Загрузка обновлений в хранилище Сервера администрирования*, *Обслуживание Сервера администрирования*, *Резервное копирование данных Сервера администрирования* и *Синхронизация обновлений Windows Update* уже созданы для Сервера администрирования, то они не отображаются в окне выбора типа задачи мастера создания задачи.

Создание задачи для набора устройств

В Kaspersky Security Center можно создавать задачи для произвольно выбранного набора устройств. Устройства в наборе могут входить в разные группы администрирования или не входить ни в одну группу администрирования. Kaspersky Security Center позволяет выполнять следующие основные задачи для набора устройств:

- Удаленная установка приложений.
- Отправка сообщения для пользователя.
- Смена Сервера администрирования.
- Управление устройствами.
- Проверка обновлений.
- Распространять инсталляционные пакеты.
- Установка приложений на подчиненные Серверы администрирования.
- Удаленная деинсталляция приложений.

Чтобы создать задачу для набора устройств:

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания одним из следующих способов:
   - В контекстном меню папки дерева консоли **Задачи** выберите пункт **Создать → Задачу**.
   - В рабочей области папки **Создать задачу** нажмите на кнопку **Задачи**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

Создание локальной задачи

Чтобы создать локальную задачу для устройства:

1. В рабочей области группы, в состав которой входит устройство, выберите вкладку **Устройства**.
2. В списке устройств на вкладке **Устройства** выберите устройство, для которого нужно создать локальную задачу.
3. Запустите процесс создания задачи для выбранного устройства одним из следующих способов:
   - Нажмите на кнопку **Выполнить действие** и в раскрывающемся списке выберите значение **Создать задачу**.
   - В рабочей области устройства перейдите по ссылке **Создать задачу**.
   - Используйте свойства устройства следующим образом:
     a. В контекстном меню устройства выберите пункт **Свойства**.
     b. В открывшемся окне свойств устройства выберите раздел **Задачи** и нажмите на кнопку **Добавить**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

Подробные описания создания и настройки локальных задач приводятся в Руководствах к соответствующим приложениям "Лаборатории Касперского".

Отображение унаследованной групповой задачи в рабочей области вложенной группы

Чтобы включить отображение унаследованных задач вложенной группы в рабочей области:

1. Выберите в рабочей области вложенной группы вкладку **Задачи**.
2. В рабочей области вкладки **Задачи** нажмите на кнопку **Показывать унаследованные задачи**.

В результате унаследованные задачи отображаются в списке задач со значком:

-  – если они были унаследованы от группы, созданной на главном Сервере администрирования;
-  – если они были унаследованы от группы верхнего уровня.

При включенном режиме наследования редактирование унаследованных задач доступно только в той группе, в которой они были созданы. Редактирование унаследованных задач недоступно в той группе, которая наследует задачи.

Автоматическое включение устройств перед запуском задачи

Kaspersky Security Center не выполняет задачи на выключенных устройствах. Вы можете настроить Kaspersky Security Center на автоматическое включение этих устройств перед запуском задачи с помощью функции Wake-on-LAN.

Чтобы настроить автоматическое включение устройств перед запуском задачи:

1. В окне свойств задачи выберите раздел **Расписание**.
2. Чтобы настроить действия на устройствах, перейдите по ссылке **Дополнительно**.
3. В открывшемся окне **Дополнительно** установите флажок **Активировать устройства перед запуском задачи функцией Wake-on-LAN за (мин)** и укажите время в минутах.

В результате за указанное количество минут до запуска задачи Kaspersky Security Center включает устройства и загружает на них операционную систему с помощью функции Wake-on-LAN. После выполнения задачи устройства автоматически выключаются, если пользователи устройств не входят в систему. Обратите внимание, что Kaspersky Security Center автоматически выключает только те устройства, которые включены с помощью функции Wake-on-LAN.

Kaspersky Security Center может автоматически запускать операционные системы только на устройствах, поддерживающих стандарт Wake-on-LAN (WoL).

Автоматическое выключение устройства после выполнения задачи

Kaspersky Security Center позволяет настроить параметры задачи таким образом, чтобы после ее выполнения устройства, на которые она распространяется, автоматически выключались.

Чтобы устройства автоматически выключались после выполнения задачи:

1. В окне свойств задачи выберите раздел **Расписание**.
2. Откройте окно настройки действий с устройствами по ссылке **Дополнительно**.
3. В открывшемся окне **Дополнительно** установите флажок **Выключать устройства после выполнения задачи**.

Ограничение времени выполнения задачи

Чтобы ограничить время выполнения задачи на устройствах:

1. В окне свойств задачи выберите раздел **Расписание**.
2. Откройте окно настройки действий с клиентскими устройствами по ссылке **Дополнительно**.
3. В открывшемся окне **Дополнительно** установите флажок **Остановить, если задача выполняется дольше (мин)** и укажите время в минутах.

В результате, если по истечении указанного времени выполнение задачи на устройстве не будет завершено, Kaspersky Security Center автоматически остановит выполнение задачи.

Экспорт задачи

Вы можете экспортировать групповые задачи и задачи для наборов устройств в файл. Задачи Сервера администрирования недоступны для экспорта.

Чтобы экспортировать задачу:

1. В контекстном меню задачи выберите пункт **Все задачи** → **Экспортировать**.
2. В открывшемся окне **Сохранить как** укажите имя файла и путь для сохранения.
3. Нажмите на кнопку **Сохранить**.

Права локальных пользователей не экспортируются.

Импорт задачи

Вы можете импортировать групповые задачи и задачи для наборов устройств. Задачи Сервера администрирования недоступны для импорта.

Чтобы импортировать задачу:

1. Выберите список задач, в который требуется импортировать задачу:
   - Если вы хотите импортировать задачу в список групповых задач, в рабочей области нужной вам группы администрирования выберите вкладку **Задачи**.
   - Если вы хотите импортировать задачу в список задач для наборов устройств, в дереве консоли выберите папку **Задачи**.
2. Выберите один из следующих способов импорта задачи:
   - В контекстном меню списка задач выберите пункт **Все задачи** → **Импортировать**.
   - По ссылке **Импортировать задачу из файла** в блоке управления списком задач.
3. В открывшемся окне укажите путь к файлу, из которого вы хотите импортировать задачу.
4. Нажмите на кнопку **Открыть**.

   В результате импортированная задача отобразится в списке задач.

Если имя новой импортированной задачи идентично имени существующей задачи, имя импортированной задачи расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Конвертация задач

С помощью Kaspersky Security Center можно конвертировать задачи предыдущих версий приложений "Лаборатории Касперского" в задачи текущих версий приложений.

Конвертация возможна для задач следующих приложений:

- Антивирус Касперского 6.0 для Windows Workstations MP4
- Kaspersky Endpoint Security 8 для Windows
- Kaspersky Endpoint Security 10 для Windows

Чтобы конвертировать задачи:

1. В дереве консоли выберите Сервер администрирования, для которого вы хотите выполнить конвертацию задач.
2. В контекстном меню Сервера администрирования выберите пункт **Все задачи** → **Мастер массовой конвертации политик и задач**.

   В результате запускается мастер массовой конвертации политик и задач. Следуйте далее указаниям мастера.

В результате работы мастера формируются новые задачи, использующие параметры задач предыдущих версий приложений.

Запуск и остановка задачи вручную

Задачи можно запускать и останавливать двумя способами: из контекстного меню задачи и в окне свойств клиентского устройства, которому назначена эта задача.

Запускать групповые задачи из контекстного меню устройства могут пользователи, входящие в группу KLAdmins.

Чтобы запустить или остановить задачу из контекстного меню или окна свойств задачи:

1. В списке задач выберите задачу.
2. Запустите или остановите задачу одним из следующих способов:
   - В контекстном меню задачи выберите пункт **Запустить** или **Остановить**.
   - В разделе **Общие** окна свойств задачи нажмите на кнопку **Запустить** или **Остановить**.

Чтобы запустить или остановить задачу из контекстного меню или окна свойств клиентского устройства:

1. В списке устройств выберите устройство.
2. Запустите или остановите задачу одним из следующих способов:
   - В контекстном меню устройства выберите пункт **Все задачи** → **Запустить задачу**. Из списка задач выберите требуемую.

     Список устройств, для которых назначена задача, будет замещен выбранным устройством. Задача будет запущена.
   - В окне свойств устройства в разделе **Задачи** нажмите на кнопку запуска () или остановки ().

Приостановка и возобновление задачи вручную

Чтобы приостановить или возобновить выполнение запущенной задачи:

1. В списке задач выберите задачу.
2. Приостановите или возобновите выполнение задачи одним из следующих способов:
   - В контекстном меню задачи выберите пункт **Приостановить** или **Возобновить**.
   - В разделе **Общие** окна свойств задачи нажмите на кнопку **Приостановить** или **Возобновить**.

Наблюдение за ходом выполнения задачи

Чтобы наблюдать за ходом выполнения задачи,

в окне свойств задачи выберите раздел **Общие**.

В средней части окна раздела **Общие** содержится информация о текущем состоянии задачи.

Просмотр результатов выполнения задач, хранящихся на Сервере администрирования

Kaspersky Security Center позволяет просматривать результаты выполнения групповых задач, задач для наборов устройств и задач Сервера администрирования.

Чтобы посмотреть результаты выполнения задачи:

в окне свойств задачи перейдите на вкладку **Результаты.**

Чтобы просмотреть результаты задачи для подчиненного Сервера администрирования:

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.
3. Нажмите на **Статистика подчиненного Сервера**.
4. Выберите подчиненный Сервер, для которого вы хотите отобразить окно **Результаты выполнения задачи**.

Настройка фильтра информации о результатах выполнения задачи

Kaspersky Security Center позволяет фильтровать информацию о результатах выполнения групповых задач, задач для наборов устройств и задач Сервера администрирования. Для локальных задач фильтрация недоступна.

Чтобы настроить фильтр для информации о результатах выполнения задачи:

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.

   Таблица в верхней части окна содержит список всех устройств, для которых назначена задача. Таблица в нижней части окна содержит результаты выполнения задачи на выбранном устройстве.
3. В интересующей вас таблице по правой клавише мыши откройте контекстное меню и выберите в нем пункт **Фильтр**.
4. В открывшемся окне **Применить фильтр** настройте параметры фильтра в разделах окна **События**, **Устройства** и **Время**. Нажмите на кнопку **ОК**.

В результате в окне **Результаты выполнения задачи** будет отображаться информация, удовлетворяющая параметрам, заданным в фильтре.

Изменение задачи. Откат изменений

Чтобы изменить задачу:

1. В дереве консоли выберите папку **Задачи**.
2. В рабочей области папки **Задачи** выберите задачу и с помощью контекстного меню перейдите в окно свойств задачи.
3. Внесите необходимые изменения.

   > В разделе **Исключения из области действия задачи** можно настроить список вложенных групп, на которые не будет распространяться задача.
4. Нажмите на кнопку **Применить**.

Изменения задачи будут сохранены в окне свойств задачи, в разделе **История ревизий**.

В случае необходимости вы можете откатить изменения задачи.

Чтобы откатить изменения задачи:

1. В дереве консоли выберите папку **Задачи**.
2. Выберите задачу, изменения которой нужно откатить и с помощью контекстного меню перейдите в окно свойств задачи.
3. В окне свойств задачи выберите раздел **История ревизий**.
4. В списке ревизий задачи выберите номер ревизии, к которой нужно откатить изменения.
5. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Откатить**.

Сравнение задач

Вы можете сравнивать задачи одного типа, например, можно сравнить две задачи поиска вредоносного ПО, но невозможно сравнить задачу поиска вредоносного ПО с задачей установки обновлений. В результате сравнения задач вы получаете отчет, показывающий, какие параметры задач совпадают, а какие различаются. Вы можете распечатать отчет сравнения задач или сохранить его в файле. Сравнение задач может потребоваться в случае, когда для разных подразделений одной компании есть различные задачи одного типа. Например, для бухгалтерии есть задача поиска вредоносного ПО только на локальных дисках устройства, а для отдела продаж, сотрудники которого переписываются с клиентами, есть задача проверять и локальные диски, и почту. Чтобы быстро увидеть такие различия, нет необходимости просматривать все параметры задачи, достаточно выполнить сравнение задач.

Сравнение можно выполнить только для задач одного типа.

Задачи можно сравнивать только попарно.

Вы можете сравнивать задачи одним из следующих способов: путем выбора одной задачи и сравнения ее с другой или путем сравнения любых двух задач из списка задач.

Чтобы выбрать одну задачу и сравнить ее с другой:

1. В дереве консоли выберите папку **Задачи**.
2. В рабочей области папки **Задачи** выберите задачу, которую нужно сравнить с другой задачей.
3. В контекстном меню задачи выберите пункт **Все задачи → Сравнить с другой задачей**.
4. В окне **Выбор задачи** выберите задачу для сравнения.
5. Нажмите на кнопку **OK**.

   Отобразится отчет сравнения двух задач в формате HTML.

Чтобы сравнить две задачи из списка задач:

1. В дереве консоли выберите папку **Задачи**.
2. В папке **Задачи** в списке задач с помощью клавиши **SHIFT** или **CTRL** выберите две задачи одного типа.
3. В контекстном меню выберите пункт **Сравнить**.

   Отобразится отчет сравнения выбранных задач в формате HTML.

При сравнении задач, в случае если используемые пароли отличаются, в отчете сравнения задач будут отображаться символы ******.

Если в свойствах задачи был изменен пароль, в отчете сравнения ревизий задачи будут отображаться символы ******.

Учетные записи для запуска задач

Вы можете задавать учетную запись, под которой должна запускаться задача.

Например, для выполнения задач проверки по требованию необходимы права на доступ к проверяемому объекту, а для выполнения задач обновления – права авторизованного пользователя прокси-сервера. Возможность задать учетную запись для запуска задачи позволяет избежать ошибки при выполнении задач проверки по требованию и задач обновления, если у пользователя, запустившего задачу, нет необходимых прав доступа.

В задачах удаленной установки и деинсталляции приложения учетная запись используется для загрузки на клиентские устройства файлов, необходимых для установки (удаления), если на устройстве не установлен или недоступен Агент администрирования. При установленном и доступном Агенте администрирования учетная запись используется, если согласно параметрам задачи доставка файлов выполняется только средствами Microsoft Windows из папки общего доступа. В этом случае учетная запись должна обладать следующими правами на устройстве:

- правом на удаленный запуск приложений;
- правами на ресурс Admin$;
- правом *Вход в качестве службы*.

Если доставку файлов на устройства выполняет Агент администрирования, учетная запись использоваться не будет. Все операции по копированию и установке файлов будет выполнять **Агент администрирования** (**Учетная запись LocalSystem**).

Экспорт результатов выполнения задачи

Если возникнут проблемы с задачей, вам, возможно, придется исследовать причины. Для анализа вы можете экспортировать результаты выполнения задачи.

Чтобы экспортировать результаты выполнения задачи:

1. Создайте пустой TXT-файл в папке на вашем устройстве.

   Результаты выполнения задачи будут экспортированы в этот файл.

2. Откройте окно с результатами выполнения задачи.

3. В верхней части окна результатов выполнения задачи выберите устройство, с которым возникли проблемы.

4. В нижней части окна результатов выполнения задачи, где отображается ход выполнения задачи для выбранного устройства, выберите одно или несколько событий.

   Чтобы выбрать несколько событий, используйте клавиши **`Shift`** или **`Ctrl`**.

5. В контекстном меню выбранного события (или событий) выберите пункт **Экспортировать**.

   В результате запустится мастер экспорта событий.

6. На шаге мастера **Файл экспорта** нажмите на кнопку **Обзор** и выберите TXT-файл, который вы создали для экспорта результатов выполнения задачи.

Если вы хотите экспортировать только выбранные события, включите параметр **Экспортировать только выбранные события**.

Если вы хотите экспортировать все результаты выполнения задачи (все события), параметр **Экспортировать только выбранные события** должен быть выключен.

7. Нажмите на кнопку **Далее**.

8. На шаге мастера **Формат экспорта** включите один из следующих параметров:

   - **Экспортировать как текст в формате Юникод, разделенный знаками табуляции**

     Включите этот параметр, если экспортируемые данные включают специальные символы, символы из нескольких языков и вам нужно быть уверенным, что все символы сохраняются точно, когда файл TXT с экспортированными данными открывается в различных приложениях.

   - **Экспортировать как текст, разделенный знаками табуляции**

     Включите этот параметр, если вы хотите сохранить совместимость со старыми системами или приложениями, которые могут не поддерживать Юникод.

9. Нажмите на кнопку **Далее**, чтобы закрыть окно мастера.

Результаты выполнения задачи экспортированы в выбранный TXT-файл.

Мастер изменения паролей задач

Для не-локальной задачи, можно указать учетную запись, с правами которой будет запускаться задача. Учетную запись можно указать во время создания задачи или в свойствах существующей задачи. Если указанная учетная запись используется в соответствии с правилами безопасности, установленными в организации, эти правила могут требовать периодического изменения пароля учетной записи. После истечения срока действия пароля учетной записи и задания нового пароля, задача не будет запускаться до тех пор, пока вы не укажете новый действующий пароль в свойствах задачи.

Мастер изменения паролей задач позволяет автоматически заменить старый пароль на новый во всех задачах, в которых указана учетная запись. Вы также можете сделать это вручную в свойствах каждой задачи.

Чтобы запустить мастер изменения паролей задач

1. В дереве консоли выберите узел **Задачи**.

2. В контекстном меню узла Сервера администрирования выберите пункт **Мастер изменения паролей задач**.

Следуйте далее указаниям мастера.

Шаг 1. Выбор учетных данных

В полях **Учетная запись** и **Пароль** укажите новые учетные данные, действующие в вашей системе (например, в Active Directory). При переходе на следующий шаг мастера, Kaspersky Security Center проверяет, совпадает ли имя указанной учетной записи с именем учетной записи в свойствах каждой не-локальной задачи. Если имена учетных записей совпадают, пароль в свойствах задачи автоматически меняется на новый.

При заполнении поля **Старый пароль (необязательно)** Kaspersky Security Center заменит пароль только для тех задач, для которых совпадают значения имени и старого пароля. Замена выполняется автоматически. Во всех остальных случаях необходимо выбрать действие, выполняемое на следующем шаге мастера.

Шаг 2. Выбор выполняемого действия

Если на первом шаге мастера вы не указали старый пароль или указанный старый пароль не соответствует паролям задач, необходимо выбрать действие, выполняемое с этими задачами.

Для каждой задачи со статусом *Требуется одобрение* определите, хотите ли вы удалить пароль в свойствах задачи или заменить его на новый. Если вы выберите удаление пароля, задача перейдет в режим запуска с правами учетной записи, заданной по умолчанию.

Шаг 3. Просмотр результатов

На последнем шаге мастера просмотрите результаты для каждой из обнаруженных задач. Для завершения работы мастера нажмите на кнопку **Готово**.

Создание иерархии групп администрирования, подчиненных виртуальному Серверу администрирования

После создания виртуального Сервера администрирования он по умолчанию содержит группу администрирования **Управляемые устройства**.

Процедура создания иерархии групп администрирования, подчиненных виртуальному Серверу администрирования, совпадает с процедурой создания иерархии групп администрирования, подчиненных физическому Серверу администрирования.

> В состав групп администрирования, подчиненных виртуальному Серверу администрирования, невозможно добавлять подчиненные и виртуальные Серверы администрирования. Это связано с ограничениями виртуальных Серверов администрирования.

Политики и профили политик

В Kaspersky Security Center Web Console можно создавать политики для приложений "Лаборатории Касперского". В этом разделе описаны политики и профили политик, а также приведены инструкции по их созданию и изменению.

Иерархия политик, использование профилей политик

В этом разделе содержится информация об особенностях применения политик к устройствам в группах администрирования. В этом разделе также содержится информация о профилях политик.

Иерархия политик

В Kaspersky Security Center политики предназначены для задания одинакового набора параметров на множестве устройств. Например, областью действия политики приложения P, определенной для группы G, являются управляемые устройства с установленным приложением P, размещенные в группе администрирования G и всех ее подгруппах, исключая те подгруппы, в свойствах которых снят флажок **Наследовать из родительской группы**.

Политика отличается от локальных параметров наличием "замков" (🔒) возле содержащихся в ней параметров. Установленный замок в свойствах политики означает, что соответствующий ему параметр (или группа параметров) должен, во-первых, быть использован при формировании эффективных параметров, во-вторых, должен быть записан в нижележащую политику.

Формирование на устройстве действующих параметров можно представить следующим образом: из политики берутся значения параметров с неустановленным замком, затем поверх них записываются значения локальных параметров, затем поверх полученных значений записываются взятые из политики значения параметров с установленным замком.

Политики одного и того же приложения действуют друг на друга по иерархии групп администрирования: параметры с установленным замком из вышележащей политики переписывают одноименные параметры из нижележащей политики.

Существует особый вид политики – политика для автономных пользователей. Эта политика вступает в силу на устройстве, когда устройство переходит в автономный режим. Политики для автономных пользователей не действуют по иерархии групп администрирования на другие политики.

Профили политик

Применение политик к устройствам, исходя только из иерархии групп администрирования, во многих случаях неудобно. Может возникнуть необходимость создать несколько копий политики для разных групп администрирования и в дальнейшем вручную синхронизировать содержимое этих политик.

Чтобы помочь избежать подобных проблем, Kaspersky Security Center поддерживает *профили политик*. Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на клиентском устройстве (компьютере, мобильном устройстве). При активации профиля изменяются параметры политики, действовавшие на устройстве до активации профиля. Эти параметры принимают значения, указанные в профиле.

Профили политик сейчас имеют следующие ограничения:

- в политике может быть не более 100 профилей;
- профиль политики не может содержать другие профили;
- профиль политики не может содержать параметры уведомлений.

Состав профиля

Профиль политики содержит следующие составные части:

- Имя. Профили с одинаковыми именами действуют друг на друга по иерархии групп администрирования с общим правилами.
- Подмножество параметров политики. В отличие от политики, где содержатся все параметры, в профиле присутствуют лишь те параметры, которые действительно нужны (на которых установлен замок).
- Условие активации – логическое выражение над свойствами устройства. Профиль активен (дополняет политику), только когда условие активации профиля становится истинным. В остальных случаях профиль неактивен и игнорируется. В логическом выражении могут участвовать следующие свойства устройства:
  - состояние автономного режима;
  - свойства сетевого окружения – имя активного правила подключения Агента администрирования;
  - наличие или отсутствие у устройства указанных тегов;
  - местоположение устройства в подразделении Active Directory: явное (устройство находится непосредственно в указанном подразделении) или неявное (устройство находится в подразделении, которое находится внутри указанного подразделения на любом уровне вложенности);
  - членство устройства в группе безопасности Active Directory (явное или неявное);
  - членство владельца устройства в группе безопасности Active Directory (явное или неявное).
- Флажок отключения профиля. Выключенные профили всегда игнорируются, условия их активации не проверяются.
- Приоритет профиля. Условия активации профилей независимы, поэтому одновременно могут активироваться сразу несколько профилей. Если активные профили содержат непересекающиеся наборы параметров, то никаких проблем не возникает. Но если два активных профиля содержат разные значения одного и того же параметра, возникает неоднозначность. Значение неоднозначной переменной будет взято из профиля с большим приоритетом (из того профиля, который располагается выше в списке профилей).

Поведение профилей при действии политик друг на друга по иерархии

Одноименные профили объединяются согласно правилам объединения политик. Профили верхней политики приоритетнее профилей нижней политики. Если в "верхней" политике запрещено изменение параметров (кнопка замок нажата), в "нижней" политике используются условия активации профиля из "верхней" политики. Если в "верхней" политике разрешено изменение параметров, то используются условия активации профиля из "нижней" политики.

Поскольку профиль политики может в условии активации содержать свойство **Устройство в автономном режиме**, профили полностью заменяют функциональность политик для автономных пользователей, которая в дальнейшем не будет поддерживаться.

Политика для автономных пользователей может содержать профили, но активация ее профилей может произойти не ранее, чем устройство перейдет в автономный режим.

Наследование параметров политики

Политика задается для группы администрирования. Параметры политики могут *наследоваться*, то есть передаваться в подгруппы (дочерние группы) групп администрирования, для которых она создана. Политика, созданная для родительской группы, также называется *родительской политикой*.

Можно включить или выключить два параметра наследования: **Наследовать параметры родительской политики** и **Форсировать наследование параметров дочерними политиками**:

- Если вы включили **Наследовать параметры родительской политики** для дочерней политики и заблокировали некоторые параметры в родительской политике, тогда вы не можете изменить эти параметры для дочерней группы. Однако вы можете изменить параметры, которые не заблокированы в родительской политике.

- Если вы выключили **Наследовать параметры родительской политики** для дочерней политики, тогда вы можете изменить все параметры в дочерней группе, даже если некоторые параметры заблокированы в родительской политике.

- Если в родительской группе включен параметр **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.

- В политиках для группы **Управляемые устройства** параметр **Наследовать параметры родительской политики** не влияет ни на какие параметры, так как группа **Управляемые устройства** не имеет вышестоящих групп и, следовательно, не наследует никакие политики.

По умолчанию параметр **Наследовать параметры родительской политики** включен для новой политики.

Если у политики имеются профили, все дочерние политики наследуют эти профили.

Управление политиками

Централизованная настройка параметров приложений, установленных на клиентских устройствах, осуществляется через определение политик.

Политики, сформированные для приложений в группе администрирования, отображаются в рабочей области на вкладке **Политики**. Перед именем каждой политики отображается значок, характеризующий ее статус.

После удаления политики или прекращения ее действия приложение продолжает работу с параметрами, заданными в политике. В дальнейшем эти параметры можно изменить вручную.

Применение политики производится следующим образом: если на устройстве выполняются резидентные задачи (задачи постоянной защиты), их выполнение продолжается с новыми значениями параметров. Запущенные периодические задачи (проверка по требованию, обновление баз приложений) выполняются с неизмененными значениями. Новый запуск периодических задач производится с измененными значениями параметров.

Политики для приложений с поддержкой мультитенантности наследуются для групп администрирования более низкого уровня, а также для групп администрирования верхнего уровня: политика распространяется на все клиентские устройства, на которых установлено приложение.

В случае использования иерархической структуры Серверов администрирования подчиненные Серверы получают политики с главного Сервера администрирования и распространяют их на клиентские устройства. При включенном механизме наследования параметры политики можно изменять на главном Сервере администрирования. После этого изменения, внесенные в параметры политики, распространяются на унаследованные политики на подчиненных Серверах администрирования.

При разрыве соединения между главным и подчиненным Серверами администрирования политика на подчиненном Сервере продолжает действовать с прежними параметрами. Параметры политики, измененные на главном Сервере администрирования, распространятся на подчиненный Сервер после восстановления соединения.

При отключенном механизме наследования параметры политики можно изменять на подчиненном Сервере независимо от главного Сервера.

Если происходит разрыв соединения между Сервером администрирования и клиентским устройством, на устройстве вступает в силу политика для автономного пользователя (если она определена), или политика продолжает действовать с прежними параметрами до восстановления соединения.

Результаты распространения политики на подчиненные Серверы администрирования отображаются в окне свойств политики на главном Сервере администрирования.

Результаты распространения политики на клиентские устройства отображаются в окне свойств политики Сервера администрирования, к которому они подключены.

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

Создание политики

В Консоли администрирования можно создавать политики непосредственно в папке группы администрирования, для которой создается политика, и в рабочей области папки **Политики**.

Чтобы создать политику в папке группы администрирования:

1. В дереве консоли выберите группу администрирования, для которой нужно создать политику.
2. В рабочей области группы выберите вкладку **Политики**.
3. Запустите мастер создания политики по кнопке **Новая политика**.

   В результате запускается мастер создания политики. Следуйте далее указаниям мастера.

*Чтобы создать политику в рабочей области папки **Политики**:*

1. В дереве консоли выберите папку **Политики**.
2. Запустите мастер создания политики по кнопке **Новая политика**.

   В результате запускается мастер создания политики. Следуйте далее указаниям мастера.

Для одного приложения в группе можно создать несколько политик, но активной может быть только одна из них. При создании новой активной политики предыдущая активная политика становится неактивной.

При создании политики можно настроить минимальный набор параметров, без которых приложение не будет работать. Остальные значения параметров устанавливаются по умолчанию и соответствуют значениям по умолчанию при локальной установке приложения. Вы можете изменять политику после ее создания.

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

Параметры приложений "Лаборатории Касперского", которые изменяются после применения политик, подробно описаны в руководствах к каждой из них.

После создания политики параметры, на изменение которых наложен запрет (установлен "замок" ( )), начинают действовать на клиентских устройствах независимо от того, какие параметры были определены для приложения ранее.

Отображение унаследованной политики во вложенной группе

Чтобы включить отображение унаследованных политик для вложенной группы администрирования:

1. В дереве консоли выберите группу администрирования, для которой нужно отображать унаследованные политики.
2. В рабочей области выбранной группы выберите вкладку **Политики**.
3. В контекстном меню списка политик выберите пункт **Вид** → **Унаследованные политики**.

   В результате унаследованные политики отображаются в списке политик со значком:

- – если они были унаследованы от группы, созданной на главном Сервере администрирования;
- – если они были унаследованы от группы верхнего уровня.

  При включенном режиме наследования параметров изменение унаследованных политик доступно только в той группе, в которой они были созданы. Изменение унаследованных политик недоступно в той группе, которая наследует политики.

Активация политики

Чтобы сделать политику активной для выбранной группы:

1. В рабочей области группы на вкладке **Политики** выберите политику, которую нужно сделать активной.
2. Для активации политики выполните одно из следующих действий:
   - В контекстном меню политики выберите пункт **Активная политика**.
   - В окне свойств политики откройте раздел **Общие** и в блоке параметров **Состояние политики** выберите вариант **Активная политика**.

В результате политика становится активной для выбранной группы администрирования.

При применении политики на большом количестве клиентских устройств на некоторое время существенно возрастают нагрузка на Сервер администрирования и объем сетевого трафика.

Автоматическая активация политики по событию "Вирусная атака"

Чтобы политика активировалась автоматически при наступлении события "Вирусная атака":

1. В окне свойств Сервера администрирования откройте раздел **Вирусная атака**.
2. Откройте окно **Активация политик** по ссылке **Настроить активацию политик по возникновению события "Вирусная атака"** и добавьте политику в выбранный список политик, активируемых при обнаружении вирусной атаки.

   В случае активации политики по событию *Вирусная атака* вернуться к предыдущей политике можно только вручную.

Применение политики для автономных пользователей

Политика для автономных пользователей вступает в силу на устройстве в случае его отключения от сети организации.

Чтобы применить политику для автономных пользователей:

в окне свойств политики откройте раздел **Общие** и в блоке параметров **Состояние политики** выберите вариант **Политика для автономных пользователей**.

В результате политика для автономных пользователей начинает действовать на устройствах в случае их отключения от сети организации.

Изменение политики. Откат изменений

Чтобы изменить политику:

1. В дереве консоли выберите папку **Политики**.
2. В рабочей области папки **Политики** выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
3. Внесите необходимые изменения.
4. Нажмите на кнопку **Применить**.

Изменения политики будут сохранены в свойствах политики, в разделе **История ревизий**.

В случае необходимости вы можете откатить изменения политики.

Чтобы откатить изменения политики:

1. В дереве консоли выберите папку **Политики**.
2. Выберите политику, изменения которой нужно откатить и с помощью контекстного меню перейдите в окно свойств политики.
3. В окне свойств политики выберите раздел **История ревизий**.
4. В списке ревизий политики выберите номер ревизии, к которой нужно откатить изменения.
5. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Откатить**.

Сравнение политик

Вы можете сравнивать две политики для одного управляемого приложения. В результате сравнения политик вы получаете отчет, показывающий, какие параметры политик совпадают, а какие различаются. Сравнивать политики бывает нужно, например, если разные администраторы в своих локальных офисах создали несколько политик для одного управляемого приложения или если одна политика верхнего уровня была унаследована и изменена для каждого локального офиса. Вы можете сравнивать политики одним из следующих способов: путем выбора одной политики и сравнения ее с другой или путем сравнения любых двух политик из списка политик.

Вы можете сравнивать только те политики, у которых есть текущие ревизии в истории ревизий.

Чтобы сравнить политику с другой политикой:

1. В дереве консоли выберите папку **Политики**.
2. В рабочей области папки **Политики** выберите политику, которую нужно сравнить с другой политикой.
3. В контекстном меню политики выберите пункт **Сравнить политику с другой политикой**.

4. В окне **Выбор политики** выберите политику, с которой нужно провести сравнение.

5. Нажмите на кнопку **OK**.

Отобразится отчет сравнения двух политик для приложения в формате HTML.

Чтобы сравнить две политики из списка политик:

1. В папке **Политики** в списке политик с помощью клавиши **SHIFT** или **CTRL** выберите две политики для одного управляемого приложения.

2. В контекстном меню выберите пункт **Сравнить**.

Отобразится отчет сравнения двух политик для приложения в формате HTML.

В отчете сравнения параметров политик для приложения Kaspersky Endpoint Security для Windows выполняется также сравнение профилей политики. Результаты сравнения параметров профилей политик можно свернуть. Чтобы свернуть блок, нажмите на значок стрелки ( ) рядом с названием блока.

Просмотр диаграммы состояния применения политики

В Kaspersky Security Center вы можете просмотреть результаты применения политик на каждом устройстве.

Чтобы просмотреть статус применения политики на каждом устройстве:

1. В рабочей области группы на вкладке **Политики** выберите политику, статус применения которой вы хотите просмотреть.

   Диаграмма на правой панели отображает состояние применения политики.

2. Нажмите на кнопку **Подробнее**.

   Откроется окно **Результаты применения политики**.

   Вы можете экспортировать результаты применения политики в файлы форматов CSV или TXT.

Удаление политики

Чтобы удалить политику:

1. В рабочей области группы администрирования на вкладке **Политики** выберите политику, которую нужно удалить.

2. Удалите политику одним из следующих способов:

   - В контекстном меню политики выберите пункт **Удалить**.

   - Перейдите по ссылке **Удалить политику** в информационном окне выбранной политики.

Копирование политики

Чтобы скопировать политику:

1. В рабочей области нужной вам группы на вкладке **Политики** выберите политику.
2. В контекстном меню политики выберите пункт **Копировать**.
3. Выберите в дереве консоли группу, в которую требуется добавить политику.

   Политику можно добавить в ту же группу, из которой она скопирована.
4. В контекстном меню списка политик для выбранной группы на вкладке **Политики** выберите пункт **Вставить**.

В результате политика копируется с сохранением всех параметров и распространяется на устройства группы, в которую она перенесена. Если вы вставляете политику в ту же группу, из которой она была скопирована, индекс **(<следующий порядковый номер>)** автоматически добавляется к имени политики, например: **(1)**, **(2)**.

Активная политика при копировании становится неактивной. В случае необходимости вы можете сделать ее активной.

Экспорт политики

Чтобы экспортировать политику:

1. Экспортируйте политику одним из следующих способов:
   - В контекстном меню политики выберите пункт **Все задачи** → **Экспортировать**.
   - Перейдите по ссылке **Экспортировать политику в файл** в информационном окне выбранной политики.
2. В открывшемся окне **Сохранить как** укажите имя файла политики и путь. Нажмите на кнопку **Сохранить**.

Импорт политики

Чтобы импортировать политику:

1. В рабочей области нужной вам группы на вкладке **Политики** выберите один из следующих способов импорта политики:
   - В контекстном меню списка политик выберите пункт **Все задачи** → **Импортировать**.
   - По кнопке **Импортировать политику из файла** в блоке управления списком политик.
2. В открывшемся окне укажите путь к файлу, из которого вы хотите импортировать политику. Нажмите на кнопку **Открыть**.

Импортированная 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)**.

Конвертация политик

Kaspersky Security Center может конвертировать политики предыдущих версий управляемых приложений "Лаборатории Касперского" в политики текущих версий этих приложений. Преобразованные политики сохраняют текущие параметры администратора, заданные до обновления, а также включают новые параметры из актуальных версий приложений. Если политика конвертирована до последней версии управляемого приложения "Лаборатории Касперского", открыть эту политику на Сервере администрирования, на котором установлена более ранняя версия плагина приложения, невозможно. Плагины управления приложениями "Лаборатории Касперского" определяют, доступна ли конвертация политик этих приложений. Информацию о преобразовании политик для каждого поддерживаемого приложения "Лаборатории Касперского" см. в соответствующей справке из следующего списка:

- **Приложения "Лаборатории Касперского" для рабочих станций:**
  - Kaspersky Endpoint Security для Windows
  - Kaspersky Endpoint Security для Linux
  - Kaspersky Endpoint Security для Linux Elbrus Edition
  - Kaspersky Endpoint Security для Mac
  - Kaspersky Endpoint Agent
  - Kaspersky Embedded Systems Security для Windows
- **Kaspersky Industrial CyberSecurity:**
  - Kaspersky Industrial CyberSecurity for Nodes
  - Kaspersky Industrial CyberSecurity for Linux Nodes
  - Kaspersky Industrial CyberSecurity for Networks (централизованное развертывание не поддерживается)
- **Приложения "Лаборатории Касперского" для мобильных устройств:**
  - Kaspersky Endpoint Security для Android
  - Kaspersky Security для iOS

- **Приложения "Лаборатории Касперского" для файловых серверов:**
  - Kaspersky Security для Windows Server
  - Kaspersky Endpoint Security для Windows
  - Kaspersky Endpoint Security для Linux
- **Приложения "Лаборатории Касперского" для виртуальных машин:**
  - Kaspersky Security для виртуальных сред Легкий агент
  - Kaspersky Security для виртуальных сред Защита без агента
- **Приложения "Лаборатории Касперского" для обнаружения целевых атак:**
  - Kaspersky Sandbox
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Managed Detection and Response
- **Приложения "Лаборатории Касперского" для устройств с операционной системой KasperskyOS:**
  - Kaspersky IoT Secure Gateway
  - Kaspersky Security Management Suite (плагин для Kaspersky Thin Client)

Чтобы конвертировать политики:

1. В дереве консоли выберите Сервер администрирования, для которого вы хотите выполнить конвертацию политик.
2. В контекстном меню Сервера администрирования выберите пункт **Все задачи → Мастер массовой конвертации политик и задач**.

   В результате запускается мастер массовой конвертации политик и задач. Следуйте далее указаниям мастера.

После завершения работы мастера создаются политики, использующие текущие параметры политик администратора и новые параметры из актуальных версий приложений "Лаборатории Касперского".

Управление профилями политик

Профиль политики – это именованный набор параметров политики, который активируется на клиентском устройстве (компьютере, мобильном устройстве), если устройство удовлетворяет заданным правилам активации. При активации профиля изменяются параметры политики, действовавшие на устройстве до активации профиля. Эти параметры принимают значения, указанные в профиле.

Профили политики нужны для того, чтобы устройства внутри одной группы администрирования могли иметь разные параметры политики. Например, возможна ситуация, когда в группе администрирования для некоторых устройств параметры политики должны быть изменены. В этом случае для такой политики можно настроить профили политики, использование которых позволяет изменять параметры политики не для всех устройств группы администрирования. Например, политика запрещает запуск приложений городской навигации для всех устройств группы администрирования "Пользователи". Приложения городской навигации необходимы для работы только одного устройства пользователя, выполняющего роль курьера, в группе администрирования "Пользователи". На этом устройстве можно установить тег "Курьер" и настроить профиль политики таким образом, чтобы был разрешен запуск приложений городской навигации только на устройстве с тегом "Курьер", с сохранением всех остальных параметров политики. В этом случае если в группе администрирования "Пользователи" появляется устройство с тегом "Курьер", на нем будет разрешен запуск приложений городской навигации. Запуск приложений городской навигации на других устройствах в группе администрирования "Пользователи", у которых тег "Курьер" отсутствует, будет запрещен.

Профили поддерживаются только для следующих политик:

- политики Kaspersky Endpoint Security для Windows;
- политики Kaspersky Endpoint Security для Mac;
- политики плагина Kaspersky Mobile Device Management версий от 10 Service Pack 1 до 10 Service Pack 3 Maintenance Release 1;
- политики плагина Kaspersky Device Management для iOS;
- политики Kaspersky Security для виртуальных сред 5.1 Легкий агент для Windows;
- политики Kaspersky Security для виртуальных сред 5.1 Легкий агент для Linux.

Профили политик облегчают управление клиентскими устройствами, на которых применены политики:

- Параметры профиля политики могут отличаться от параметров самой политики.
- Не требуется поддерживать и применять вручную несколько копий одной политики, которые различаются только небольшим количеством параметров.
- Не требуется отдельная политика для автономных пользователей.
- Вы можете экспортировать и импортировать профили политики, а также создавать новые профили на основе существующих.
- Для одной политики несколько профилей политики могут быть активными. К устройству будут применены те из профилей, которые удовлетворяют правилам активации на этом устройстве.
- Профили подчиняются иерархии политик. Унаследованная политика содержит все профили политики верхнего уровня.

Приоритеты профилей

Профили, созданные для политики, упорядочены в порядке убывания приоритета. Например, если профиль X находится выше профиля Y в списке профилей, то профиль X имеет более высокий приоритет, чем Y. К одному устройству одновременно могут быть применены несколько профилей. Если значение какого-то параметра различается в профилях, на устройстве применится значение параметра из того профиля, который имеет более высокий приоритет.

Правила активации профиля

Профиль политики активируется на клиентском устройстве при выполнении правила активации. *Правила активации* – набор условий, при выполнении которых профиль политики начинает работать на устройстве. Правило активации может содержать следующие условия:

- Агент администрирования на клиентском устройстве подключается к Серверу с определенным набором параметров подключения, например, адрес Сервера, номер порта и так далее.
- Клиентское устройство находится в автономном режиме.
- Клиентскому устройству назначены определенные теги.
- Клиентское устройство явно (устройство находится непосредственно в указанном подразделении) или неявно (устройство находится в подразделении, которое находится внутри указанного подразделения на любом уровне вложенности) размещено в определенном подразделении Active Directory®, устройство или его владелец находятся в группе безопасности Active Directory.
- Клиентское устройство принадлежит определенному владельцу или владелец устройства находится во внутренней группе безопасности Kaspersky Security Center.
- Владельцу клиентского устройства была назначена определенная роль.

Политики в иерархии групп администрирования

Если вы создаете политику в группе администрирования нижнего уровня, то новая политика наследует профили активной политики для группы верхнего уровня. Профили с одинаковыми именами объединяются. Профили политики для группы более высокого уровня имеют более высокий приоритет. Например, в группе администрирования *A* политика *P(A)* имеет профили *X1*, *X2*, и *X3*, в порядке убывания приоритета. В группе администрирования *B*, которая является подгруппой группы *A*, создана политика *P(B)*, с профилями *X2*, *X4*, *X5*. Тогда политика *P(B)* будет изменена политикой *P(A)*, так, что в политике *P(B)* список профилей в порядке убывания приоритета будет *X1*, *X2*, *X3*, *X4*, *X5*. Приоритет профиля *X2* будет зависеть от начального состояния *X2* политики *P(B)* и *X2* политики *P(A)*. После создания политики *P(B)* политика *P(A)* не будет отображаться в подгруппе *B*.

Активная политика вычисляется каждый раз заново при запуске Агента администрирования, при включении и выключении автономного режима, а также при изменении списка тегов, назначенных клиентскому устройству. Например, устройству увеличили объем оперативной памяти, в результате активировался профиль политики, который применяется для устройств с большим объемом оперативной памяти.

Свойства и ограничения профиля политики

Профили имеют следующие свойства:

- Профили неактивной политики не влияют на клиентские устройства.
- Если для политики установлено состояние **Политика для автономных пользователей**, профили политики также будут применяться при отключении устройства от корпоративной сети.

- Профили не поддерживают статический анализ доступа к исполняемым файлам.
- Профиль политики не может содержать параметры оповещений о событиях.
- Если используется UDP-порт 15000 для подключения устройства к Серверу администрирования, то при назначении тега устройству соответствующий профиль политики активируется в течение одной минуты.
- Вы можете использовать правила подключения Агента администрирования к Серверу администрирования, когда вы создаете правила активации профиля политики.

Создание профиля политики

Создание профиля доступно только для политик следующих приложений:

- Kaspersky Endpoint Security 10 Service Pack 1 для Windows и выше;
- Kaspersky Endpoint Security 10 Service Pack 1 для Mac;
- плагина Kaspersky Mobile Device Management до версий 10 Service Pack 3 Maintenance Release 1;
- плагина Kaspersky Device Management для iOS;
- Kaspersky Security для виртуальных сред 5.1 Легкий агент для Windows и Linux.

Чтобы создать профиль политики:

1. В дереве консоли выберите группу администрирования, для политики которой нужно создать профиль политики.
2. В рабочей области группы администрирования выберите вкладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Выберите раздел **Профили политики** в окне свойств политики и нажмите на кнопку **Добавить**.

   Запустится мастер создания профиля политики.
5. В окне мастера **Имя профиля политики** укажите:

   a. Имя профиля политики.

      Имя профиля не может превышать 100 символов.

   b. Состояние профиля политики (*Включен* или *Выключен*).

      Рекомендуется создавать неактивные профили политики и включать их только после полного завершения настройки параметров и условий активации профилей политики.
6. Установите флажок **После закрытия мастера создания профиля политики перейти к настройке правила активации профиля политики**, чтобы запустить мастер создания правила активации профиля политики. Следуйте инструкциям мастера.
7. Измените параметры профиля политики в окне свойств профиля политики, как вам необходимо.

8. Сохраните изменения, нажав на кнопку **OK**.

   Профиль будет сохранен. Профиль будет активирован на устройствах, удовлетворяющих правилам активации.

Для одной политики можно создать несколько профилей политики. Профили, созданные для политики, отображаются в свойствах политики в разделе **Профили политики**. Вы можете изменить профиль политики и приоритет профиля, а также удалить профиль.

Изменение профиля политики

Изменение параметров профиля политики

> Изменение профиля доступно только для политик Kaspersky Endpoint Security для Windows.

Чтобы изменить профиль политики:

1. В дереве консоли выберите группу администрирования, для которой нужно изменить профиль политики.
2. В рабочей области группы выберите вкладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Откройте раздел **Профили политики** в свойствах политики.

   В разделе содержится список профилей, созданных для политики. Профили в списке отображаются в соответствии с их приоритетом.
5. Выберите профиль политики и нажмите на кнопку **Свойства**.
6. В окне свойств настройте параметры профиля:
   - Если необходимо, в разделе **Общие** измените имя профиля и включите или выключите профиль с помощью флажка **Включить профиль**.
   - В разделе **Правила активации** измените правила активации профиля.
   - Измените параметры политики в соответствующих разделах.
7. Нажмите на кнопку **OK**.

Измененные параметры начнут действовать после синхронизации устройства с Сервером администрирования (если профиль политики активен) либо после выполнения правила активации (если профиль политики неактивен).

Изменение приоритета профиля политики

Приоритет профилей политик определяет порядок активации профилей на клиентском устройстве. Приоритет используется, если для разных профилей политики заданы одинаковые правила активации.

Например, созданы два профиля политики: *Профиль 1* и *Профиль 2*, отличающиеся друг от друга значениями одного параметра (*Значение 1* и *Значение 2*). Приоритет *Профиля 1* выше, чем приоритет *Профиля 2*. Кроме того, существуют профили с более низким приоритетом, чем *Профиль 2*. Правила активации профилей совпадают.

При выполнении правила активации будет активирован *Профиль 1*. Параметр на устройстве примет *Значение 1*. Если удалить *Профиль 1*, то *Профиль 2*, будет иметь самый высокий приоритет, и параметр примет *Значение 2*.

В списке профилей политики профили отображаются в соответствии с их приоритетом. На первом месте в списке стоит профиль с самым высоким приоритетом. Приоритет профиля можно изменять с помощью кнопок со стрелкой вверх  и со стрелкой вниз .

Удаление профиля политики

Чтобы удалить профиль политики:

1. Выберите в дереве консоли группу администрирования, для которой нужно удалить профиль политики.
2. В рабочей области группы администрирования выберите вкладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Откройте раздел **Профили политики** в свойствах политики Kaspersky Endpoint Security.
5. Выберите профиль политики, который нужно удалить, и нажмите на кнопку **Удалить**.

В результате профиль политики будет удален. Активным станет либо другой профиль политики, правила активации которого выполняются на устройстве, либо политика.

Создание правила активации профиля политики

Чтобы создать правило активации профиля политики:

1. В дереве консоли выберите группу администрирования, для которой нужно создать правило активации профиля политики.
2. В рабочей области группы выберите вкладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Выберите раздел **Профили политики** в окне свойств политики.
5. Выберите профиль политики, для которого нужно создать правило активации, и нажмите на кнопку **Свойства**.

   В результате откроется окно свойств профиля политики.

   Если список профилей политики пуст, вы можете создать профиль политики.
6. Выберите раздел **Правила активации** и нажмите на кнопку **Добавить**.

   В результате запустится мастер создания правила активации профиля политики.

7. В окне **Правила активации профиля политики** 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.

   - **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.

   - **Правила для определенного владельца устройства**

     Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от того, кто является владельцем устройства, и от членства устройства во внутренней группе безопасности Kaspersky Security Center.

   - **Правило для характеристик оборудования**

     Установите флажок, чтобы настроить условие активации профиля политики на устройстве в зависимости от объема памяти и количества логических процессоров устройства.

   От выбора параметров на этом шаге зависит дальнейшее количество окон мастера. Вы можете изменить правила активации профиля политики позже.

8. В разделе **Общие условия** укажите следующие параметры:

   - В поле **Устройство в автономном режиме** в раскрывающемся списке укажите условие нахождения устройства в сети:

     - **Да**

       Устройство находится во внешней сети, то есть Сервер администрирования недоступен.

     - **Нет**

       Устройство находится в сети, Сервер администрирования доступен.

     - **Значение не выбрано**

       Критерий не применяется.

   - В поле **Устройство находится в указанном сетевом местоположении** с помощью раскрывающихся списков настройте активацию профиля политики при выполнении/невыполнении на устройстве правила подключения к Серверу администрирования:

     - **Выполняется/Не выполняется**

       Условие активации профиля политики (правило выполняется или не выполняется).

     - **Имя правила**

       Описание сетевого местоположения 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.

Окно **Общие условия** отображается, если был установлен флажок **Общие правила активации профиля политики**.

9. В разделе **Условия с использованием тегов** укажите следующие параметры:

   - **Список тегов**

     В списке тегов задайте правило включения устройств в профиль политики, установив флажки нужным тегам.

     Вы можете добавить в список новые теги, введя их в поле над списком и нажав на кнопку **Добавить**.

     В профиль политики будут включены устройства, в описании которых есть все выбранные теги. Если флажки сняты, критерий не применяется. По умолчанию флажки сняты.

   - **Применить к устройствам без выбранных тегов**

     Включите параметр, если необходимо инвертировать выбор тегов.

     Если параметр включен, в профиль политики будут включены устройства, в описании которых нет выбранных тегов. Если этот параметр выключен, критерий не применяется.

     По умолчанию параметр выключен.

   Окно **Условия с использованием тегов** отображается, если установлен флажок **Общие правила активации профиля политики**.

10. В разделе **Условия с использованием Active Directory** укажите следующие параметры:

    - **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.

    Окно **Условия с использованием Active Directory** отображается, если установлен флажок **Правила для использования Active Directory**.

11. В разделе **Условия с использованием владельца устройства** укажите следующие параметры:

- **Владелец устройства**

  Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по владельцу устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

  - устройство принадлежит указанному владельцу (знак "=");
  - устройство не принадлежит указанному владельцу (знак "#").

    Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать владельца устройства, когда параметр включен. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- **Владелец устройства входит во внутреннюю группу безопасности**

  Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по членству владельца устройства во внутренней группе безопасности Kaspersky Security Center. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

  - владелец устройства является членом указанной группы безопасности (знак "=");
  - владелец устройства не является членом указанной группы безопасности (знак "#").

    Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать группу безопасности Kaspersky Security Center. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- **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.

Окно **Условия с использованием владельца устройства** отображается, если установлен флажок **Правила для определенного владельца устройства**.

12. В разделе **Условия с использованием характеристик оборудования** укажите следующие параметры:

- **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.

Окно **Условия с использованием характеристик оборудования** отображается, если установлен флажок **Правило для характеристик оборудования**.

13. В окне **Имя правила активации профиля политики** в поле **Имя правила** укажите название правила.

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 в разделе **Правила активации**. Вы можете изменить или удалить правило активации профиля политики.

Несколько правил активации могут выполняться одновременно.

Правила перемещения устройств

Рекомендуется автоматизировать процесс размещения устройств в группах администрирования при помощи *правил перемещения устройств*. Правило перемещения состоит из трех основных частей: имени, условия выполнения (логического выражения над атрибутами устройства) и целевой группы администрирования. Правило перемещает устройство в целевую группу администрирования, если атрибуты устройства удовлетворяют условию выполнения правила.

Правила перемещения устройств имеют приоритеты. Сервер администрирования проверяет атрибуты устройства на соответствие условию выполнения каждого правила, в порядке убывания приоритета правил. Если атрибуты устройства удовлетворяют условию выполнения правила, то устройство перемещается в целевую группу, и на этом обработка правил для этого устройства прекращается. Если атрибуты устройства удовлетворяют сразу нескольким правилам, то устройство будет перемещено в целевую группу того правила, которое имеет больший приоритет (стоит в списке правил выше).

Правила перемещения устройств могут создаваться неявно. Например, в свойствах пакета или задачи удаленной установки может быть указана группа администрирования, в которую должно попасть устройство после установки на нем Агента администрирования. Также правила перемещения могут быть созданы администратором Kaspersky Security Center в явном виде, в списке правил перемещения. Список расположен в Консоли администрирования в свойствах группы **Нераспределенные устройства**.

Правило перемещения по умолчанию предназначено для однократного первоначального размещения устройств в группах администрирования. Правило перемещает только один раз устройства, находящиеся в группе **Нераспределенные устройства**. Если устройство однажды было перемещено этим правилом, правило не переместит его повторно, даже если вернуть устройство вручную в группу **Нераспределенные устройства**. Это рекомендуемый способ использования правил перемещения.

Можно перемещать устройства, уже размещенные в группах администрирования. Для этого в свойствах правила снимите флажок **Перемещать только устройства, которые не входят ни в одну группу администрирования**.

Наличие правил перемещения, действующих на устройства, уже размещенные в группах администрирования, существенно увеличивает нагрузку на Сервер администрирования.

Флажок **Перемещать только устройства, которые не входят ни в одну группу администрирования** заблокирован в свойствах автоматически созданных правил перемещения. Такие правила создаются при добавлении задачи *Удаленная установка приложения* или создании автономного инсталляционного пакета.

Можно создать правило перемещения, способное многократно действовать на одно и то же устройство.

Настоятельно рекомендуется избегать подхода к работе с управляемыми устройствами, при котором одно и то же устройство многократно перемещается из группы в группу, например, с целью применения к устройству особой политики, запуска специальной групповой задачи, обновления с определенной точки распространения.

Подобные сценарии не поддерживаются, так как они крайне неэффективны по нагрузке на Сервер администрирования и на сетевой трафик. Также эти сценарии противоречат модели работы Kaspersky Security Center (особенно в области прав доступа, событий и отчетов). Следует искать другое решение, например, использовать профили политик, задачи для выборок устройств, назначать Агенты администрирования согласно методике.

Копирование правил перемещения устройств

Если вам нужно создать несколько правил перемещения устройств с аналогичными параметрами, вы можете скопировать существующее правило, а затем изменить параметры скопированного правила. Например, это удобно, когда вам нужно иметь несколько одинаковых правил перемещения устройств с разными IP-диапазонами и целевыми группами.

Чтобы скопировать правило перемещения устройств:

1. Откройте главное окно приложения.
2. В папке **Нераспределенные устройства** нажмите на кнопку **Настроить правила**.

   Откроется окно **Свойства: Нераспределенные устройства**.
3. В разделе **Перемещение устройств** выберите правило перемещения устройств, которое вы хотите скопировать.
4. Нажмите на кнопку **Клонировать правило**.

   Копия выбранного правила будет добавлена в конец списка.

Новое правило будет создано выключенным. Вы можете выключить или изменить правило в любое время.

Категоризация программного обеспечения

Основным средством контроля запуска приложений являются *категории "Лаборатории Касперского"* (далее также *KL-категории*). KL-категории облегчают администратору Kaspersky Security Center работу по поддержанию категоризации ПО и минимизируют объем трафика, передаваемого на управляемые устройства.

Пользовательские категории следует создавать только для приложений, не подпадающих ни под одну KL-категорию (например, для приложений, разработанных на заказ). Пользовательские категории создаются на основе дистрибутива приложения (MSI) или на основе папки с дистрибутивами.

Если имеется большая пополняемая коллекция программного обеспечения, не категоризированного при помощи KL-категорий, может быть целесообразным создать автоматически обновляемую категорию. Такая категория будет автоматически пополняться контрольными суммами исполняемых файлов при изменении папки с дистрибутивами.

Не создавайте автоматически обновляемые категории программного обеспечения для папок Мои документы, %windir%, %ProgramFiles% и %ProgramFiles(x86)%. Файлы в этих папках часто меняются, что приводит к увеличению нагрузки на Сервер администрирования и к увеличению трафика в сети. Следует создать отдельную папку с коллекцией программного обеспечения и время от времени пополнять ее.

Необходимые условия для установки приложений на устройства организации-клиента

Процесс удаленной установки приложений на устройства организации-клиента совпадает с процессом удаленной установки приложений внутри организации.

Для установки приложений на устройства организации-клиента необходимо выполнение следующих условий:

- Перед первой установкой приложений на устройства организации-клиента требуется установить на них Агент администрирования.

  При настройке инсталляционного пакета Агента администрирования поставщиком услуг в приложении Kaspersky Security Center в окне свойств инсталляционного пакета требуется настроить следующие параметры:

  - В разделе **Подключение** в строке **Сервер администрирования** требуется указать тот же адрес виртуального Сервера администрирования, что и при локальной установке Агента администрирования на точку распространения.

  - В разделе **Дополнительно** установите флажок **Подключаться к Серверу администрирования через шлюз соединения**. В строке **Адрес шлюза соединения** нужно указать адрес точки распространения. В качестве адреса устройства можно использовать IP-адрес или имя устройства в сети Windows.

- В качестве способа загрузки инсталляционного пакета Агента администрирования необходимо выбрать **Средствами операционной системы с помощью точек распространения**. Выбор способа загрузки осуществляется следующим образом:

  - При установке приложений с помощью задач удаленной установки способ загрузки можно выбрать двумя способами:

    - при создании задачи удаленной установки в окне **Параметры**;

    - в окне свойств задачи удаленной установки в разделе **Параметры**.

  - При установке приложений с помощью мастера удаленной установки способ загрузки можно выбрать в окне мастера **Параметры**.

- Учетная запись, под которой работает точка распространения, должна иметь доступ к ресурсу Admin$ на клиентских устройствах.

Просмотр и изменение локальных параметров приложения

Система администрирования Kaspersky Security Center позволяет удаленно управлять локальными параметрами приложений на устройствах через Консоль администрирования.

Локальные параметры приложения – это параметры приложения, индивидуальные для устройства. Kaspersky Security Center позволяет устанавливать локальные параметры приложений для устройств, входящих в группы администрирования.

Подробные описания параметров приложений "Лаборатории Касперского" приводятся в руководствах для этих приложений.

Чтобы просмотреть или изменить локальные параметры приложения:

1. В рабочей области группы, в которую входит нужное вам устройство, выберите вкладку **Устройства**.

2. В окне свойств в разделе **Приложения** выберите соответствующее приложение.

3. Откройте окно свойств приложения двойным щелчком мыши по названию приложения или нажатием на кнопку **Свойства**.

В результате откроется окно локальных параметров выбранного приложения, которые можно просмотреть и изменить.

Вы можете изменять значения тех параметров, изменение которых не запрещено групповой политикой (параметр не закрыт замком (🔒) в политике).

Обновление Kaspersky Security Center и управляемых приложений

В этом разделе описаны шаги, которые необходимо выполнить для обновления Kaspersky Security Center и управляемых приложений.

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"

В этом разделе представлен сценарий регулярного обновления баз данных, модулей приложений и приложений "Лаборатории Касперского". После того, как вы завершили сценарий Настройка защиты в сети организации, вам нужно поддерживать надежность системы защиты, чтобы обеспечить защиту Серверов администрирования и управляемых устройств от различных угроз, включая вирусы, сетевые атаки и фишинговые атаки.

Защита сети поддерживается обновленной с помощью регулярных обновлений следующего:

- баз и модулей приложений "Лаборатории Касперского";
- установленных приложений "Лаборатории Касперского", включая компоненты Kaspersky Security Center и приложений безопасности.

Когда вы завершите этот сценарий, вы можете быть уверены, что:

- Ваша сеть защищена самым последним программным обеспечением "Лаборатории Касперского", включая компоненты Kaspersky Security Center и приложения безопасности.
- Антивирусные базы и другие базы данных "Лаборатории Касперского", критически важные для безопасности сети, всегда актуальны.

Предварительные требования

Управляемые устройства должны иметь соединение с Сервером администрирования. Если у устройств нет соединения, рассмотрите возможность обновления баз, модулей приложений и приложений "Лаборатории Касперского" вручную или напрямую с серверов обновлений "Лаборатории Касперского".

Сервер администрирования должен иметь подключение к интернету.

Прежде чем приступать, убедитесь, что вы выполнили следующее:

1. Развернуты приложения безопасности "Лаборатории Касперского" на управляемых устройствах в соответствии со сценарием развертывания приложений "Лаборатории Касперского" с помощью Kaspersky Security Center Web Console.

2. Созданы и настроены все необходимые политики, профили политик и задачи в соответствии со сценарием настройки защиты сети.

3. Назначено соответствующее количество точек распространения в соответствии с количеством управляемых устройств и топологией сети.

Обновление баз и приложений "Лаборатории Касперского" состоит из следующих этапов:

1. **Выбор схемы обновления**

   Существует несколько схем, которые вы можете использовать для установки обновлений компонентов Kaspersky Security Center и приложений безопасности. Выберите схему или несколько схем, которые лучше всего соответствуют требованиям вашей сети.

2. **Создание задачи для загрузки обновлений в хранилище Сервера администрирования**

   Эта задача автоматически создается в мастере первоначальной настройки Kaspersky Security Center. Если вы не запускали мастер первоначальной настройки, создайте задачу сейчас.

   Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования, а также обновления баз и модулей приложений для Kaspersky Security Center. После загрузки обновлений их можно распространять на управляемые устройства.

   Если в вашей сети назначены точки распространения, обновления автоматически загружаются из хранилища Сервера администрирования в хранилища точек распространения. В этом случае управляемые устройства, входящие в область действия точки распространения, загружают обновления из хранилищ точек распространения, вместо хранилища Сервера администрирования.

   Инструкции:

   - Консоль администрирования: Создание задачи для загрузки обновлений в хранилище Сервера администрирования.
   - Kaspersky Security Center Web Console: Создание задачи для загрузки обновлений в хранилище Сервера администрирования.

3. **Создание задачи загрузки обновлений в хранилища точек распространения (если требуется)**

   По умолчанию обновления загружаются в хранилища точек распространения из хранилища Сервера администрирования. Вы можете настроить Kaspersky Security Center так, чтобы точки распространения загружали обновления непосредственно с серверов обновлений "Лаборатории Касперского". Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.

   Когда вашей сети назначены точки распространения и создана задача *Загрузка обновлений в хранилища точек распространения*, точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

Инструкции:

- Консоль администрирования: Создание задачи загрузки обновлений в хранилища точек распространения.
- Kaspersky Security Center Web Console: Создание задачи загрузки обновлений в хранилища точек распространения.

4. **Настройка точек распространения**

   Если в вашей сети назначены точки распространения, убедитесь, что параметр **Распространять обновления** включен в свойствах всех требуемых точек распространения. Если этот параметр выключен для точки распространения, устройства, включенные в область действия точки распространения, загружают обновления из хранилища Сервера администрирования.

   Если вы хотите, чтобы управляемые устройства получали обновления только от точек распространения, включите параметр **Распространять файлы только через точки распространения** в политике Агента администрирования.

5. **Оптимизация процесса обновления с использованием офлайн-модели получения обновлений или загрузки файлов различий (если требуется)**

   Вы можете оптимизировать процесс обновления, используя офлайн-модель загрузки обновлений (включена по умолчанию), или используя файлы различий. Для каждого сегмента сети вам нужно выбрать, какую из этих двух функций включить, так как они не могут работать одновременно.

   Когда офлайн-модель получения обновлений включена, Агент администрирования загружает необходимые обновления на управляемое устройство после загрузки обновлений в хранилище Сервера администрирования, прежде чем приложение безопасности запросит обновления. Это повышает надежность процесса обновления. Чтобы использовать эту функцию, включите параметр **Загружать обновления и антивирусные базы с Сервера администрирования заранее (рекомендуется)** в свойствах задачи Политика Агента администрирования.

   Если вы не используете офлайн-модель загрузки обновлений, вы можете оптимизировать трафик между Сервером администрирования и управляемыми устройствами, используя файлы различий. Когда эта функция включена, Сервер администрирования или точка распространения загружает файлы различий вместо целых файлов баз данных или модулей приложений "Лаборатории Касперского". Файл различий описывает различия между двумя версиями файлов базы или модулями приложения. Поэтому файлы различий занимают меньше места, чем целые файлы. В результате уменьшается трафик между Сервером администрирования или точками распространения и управляемыми устройствами. Чтобы использовать эту функцию, включите параметр **Загрузить файлы различий** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования* и/или *Загрузка обновлений в хранилища точек распространения*.

   Инструкции:

   - Использование файлов различий для обновления баз и модулей приложений "Лаборатории Касперского".
   - Консоль администрирования: Включение и выключение офлайн-модели получения обновлений.
   - Kaspersky Security Center Web Console: Консоль администрирования: Включение и выключение офлайн-модели получения обновлений.

6. **Проверка полученных обновлений (если требуется)**

   Перед установкой загруженных обновлений вы можете проверить обновления с помощью задачи *Проверка обновлений*. Эта задача последовательно запускает задачи обновления устройства и задачи поиска вредоносного ПО, настроенные с помощью параметров для указанного набора тестовых устройств. После получения результатов задачи Сервер администрирования запустит или заблокирует распространение обновлений на оставшиеся устройства.

Задача *Проверка обновлений* может быть выполнена как часть задачи *Загрузка обновлений в хранилище Сервера администрирования*. В свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования* включите параметр **Выполнять проверку обновлений перед распространением** в Консоли администрирования или параметр **Выполнить проверку обновлений** в Kaspersky Security Center Web Console.

Инструкции:

- Консоль администрирования: Проверка полученных обновлений.
- Kaspersky Security Center Web Console: Проверка полученных обновлений.

7. **Одобрение и отклонение обновлений программного обеспечения**

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 требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства. Неопределенные обновления могут быть установлены только на Агенте администрирования и других компонентах Kaspersky Security Center в соответствии с параметрами политики Агента администрирования. Обновления, которым вы установили статус *Отклонено*, не устанавливаются на управляемые устройства. Если ранее отклоненное обновление для приложения безопасности было установлено, Kaspersky Security Center попытается удалить обновления со всех устройств.

Одобрение и отклонение обновлений доступно только для Агента администрирования и управляемых приложений "Лаборатории Касперского", установленных на клиентских устройствах под управлением Windows и Linux. Бесшовное обновление Сервера администрирования, Kaspersky Security Center Web Console и веб-плагинов управления не поддерживается.

Инструкции:

- Консоль администрирования: Одобрение и отклонение обновлений программного обеспечения.
- Kaspersky Security Center Web Console: Одобрение и отклонение обновлений программного обеспечения.

8. **Настройка автоматической установки обновлений и патчей для компонентов Kaspersky Security Center**

Загруженные обновления и патчи для Агента администрирования и других компонентов Kaspersky Security Center 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*.

Инструкции:

- Консоль администрирования: Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center.
- Kaspersky Security Center Web Console: Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center.

9. **Установка обновлений для Сервера администрирования**

   Обновления программного обеспечения для Сервера администрирования не зависят от статусов обновлений. Они не устанавливаются автоматически и должны быть предварительно одобрены администратором на вкладке **Мониторинг** в Консоли администрирования (**Сервер администрирования** `<имя Сервера>` → **Мониторинг**) или в разделе **Уведомления** в Kaspersky Security Center Web Console (**Мониторинг и отчеты** → **Уведомления**). После этого администратор должен явно запустить установку обновлений.

10. **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 выбрать параметр **При загрузке обновлений в хранилище** при настройке расписания задач для своевременного обновления.

    Если в вашей сети есть устройства, поддерживающие только IPv6, и вы хотите регулярно обновлять приложения безопасности, установленные на этих устройствах, убедитесь, что на управляемых устройствах установлены Сервер администрирования (версии 13.2 или выше) и Агент администрирования (версии 13.2 или выше).

    По умолчанию обновления для Kaspersky Endpoint Security для Windows и для Kaspersky Endpoint Security для Linux устанавливаются только после изменения статуса обновления на *Одобрено*. 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.

    Инструкции:

    - Консоль администрирования: Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства.
    - Kaspersky Security Center Web Console: Консоль администрирования: Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства.

Результаты

По завершении сценария Kaspersky Security Center настроен для обновления баз "Лаборатории Касперского" и установленных приложений "Лаборатории Касперского" после загрузки обновлений в хранилище Сервера администрирования или в хранилища точек распространения. Теперь вы можете приступить к мониторингу состояния сети.

Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"

Чтобы убедиться, что защита ваших Серверов администрирования и управляемых устройств актуальна, вам нужно своевременно предоставлять обновления следующего:

- Баз и модулей приложений "Лаборатории Касперского".

Kaspersky Security Center проверяет доступность серверов "Лаборатории Касперского" перед загрузкой баз и 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 и приложений безопасности.

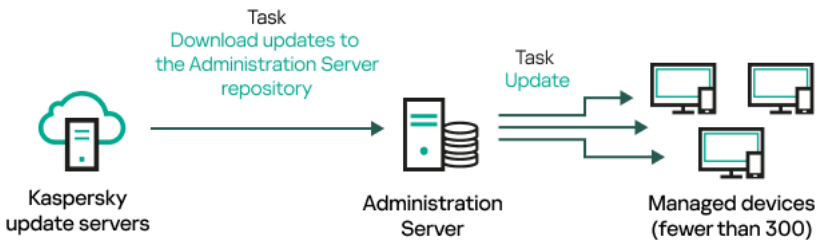
  Kaspersky Security Center позволяет автоматически обновлять Агент администрирования и приложения "Лаборатории Касперского", установленные на клиентских устройствах под управлением Windows и Linux. Бесшовное обновление Сервера администрирования, Kaspersky Security Center Web Console и веб-плагинов управления не поддерживается. Для обновления этих компонентов вам необходимо скачать их последние версии с сайта "Лаборатории Касперского" и установить их вручную.

В зависимости от конфигурации вашей сети вы можете использовать следующие схемы загрузки и распространения необходимых обновлений на управляемые устройства:

- С помощью одной задачи: *Загрузка обновлений в хранилище Сервера администрирования*
- С помощью двух задач:
  - Задача *Загрузка обновлений в хранилище Сервера администрирования*.
  - Задача *Загрузка обновлений в хранилища точек распространения*.
- Вручную через локальную папку, общую папку или FTP-сервер
- Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security на управляемых устройствах
- Через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

Использование задачи Загрузка обновлений в хранилище Сервера администрирования

В этой схеме Kaspersky Security Center загружает обновления с помощью задачи *Загрузка обновлений в хранилище Сервера администрирования*. В небольших сетях, которые содержат менее 300 управляемых устройств в одном сегменте сети или менее десяти управляемых устройств в каждом сегменте, обновления распространяются на управляемые устройства непосредственно из хранилища Сервера администрирования (см. рисунок ниже).



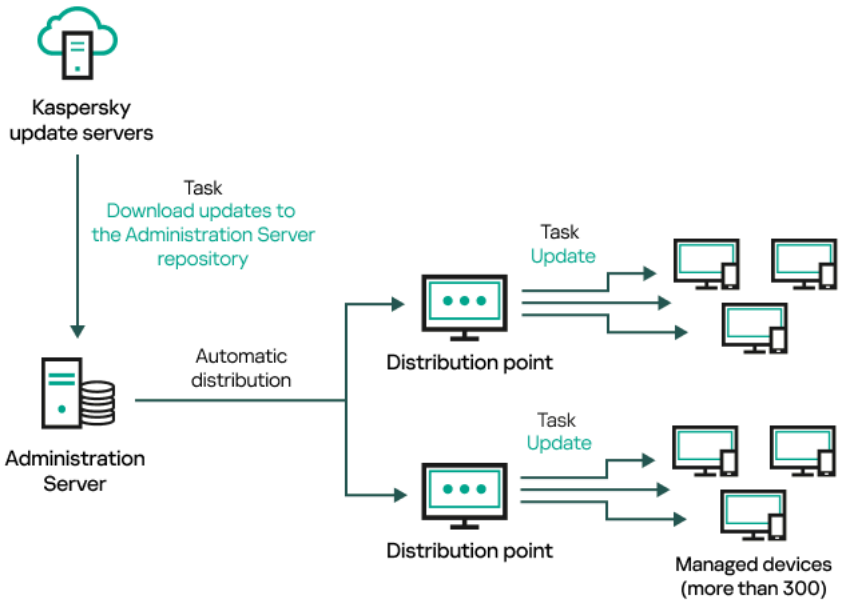
Обновление с использованием задачи Загрузка обновлений в хранилище Сервера администрирования и без точек распространения

По умолчанию Сервер администрирования взаимодействует с серверами обновлений "Лаборатории

Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.

Если ваша сеть содержит более 300 управляемых устройств в одном сегменте сети или ваша сеть содержит несколько сегментов, в которых больше девяти управляемых устройств, мы рекомендуем использовать точки распространения для распространения обновлений на управляемые устройства (см. рисунок ниже). Точки распространения уменьшают загрузку Сервера администрирования и оптимизируют трафик между Сервером администрирования и управляемыми устройствами. Вы можете рассчитать количество точек распространения и их конфигурацию, необходимые для вашей сети.

В этой схеме обновления автоматически загружаются из хранилища Сервера администрирования в хранилища точек распространения. Управляемые устройства, входящие в область действия точки распространения, загружают обновления из хранилищ точек распространения, вместо хранилища Сервера администрирования.



Обновление с использованием задачи Загрузка обновлений в хранилище Сервера администрирования с точками распространения

После завершения задачи *Загрузка обновлений в хранилище Сервера администрирования* следующие обновления загружаются в хранилище Сервера администрирования:

- Базы и модули приложений "Лаборатории Касперского" для Kaspersky Security Center.

  Эти обновления устанавливаются автоматически.

- 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 Сервера администрирования.

  Эти обновления не устанавливаются автоматически. Администратор должен явно одобрить обновления и запустить установку обновлений.

  Для установки патчей на Сервере администрирования требуются права локального администратора.

- Обновления для компонентов Kaspersky Security Center.

  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. (Вы можете одобрить обновления с помощью Консоли администрирования или Kaspersky Security Center Web Console). Обновления устанавливаются с помощью задачи *Обновление* и могут быть настроены в свойствах этой задачи.

Задача *Загрузка обновлений в хранилище Сервера администрирования* недоступна на виртуальных Серверах администрирования. В хранилище виртуального Сервера отображаются обновления, загруженные на главный Сервер администрирования.

Вы можете настроить проверку полученных обновлений на работоспособность и на наличие ошибок на наборе тестовых устройств. Если проверка прошла успешно, обновления распространяются на другие управляемые устройства.

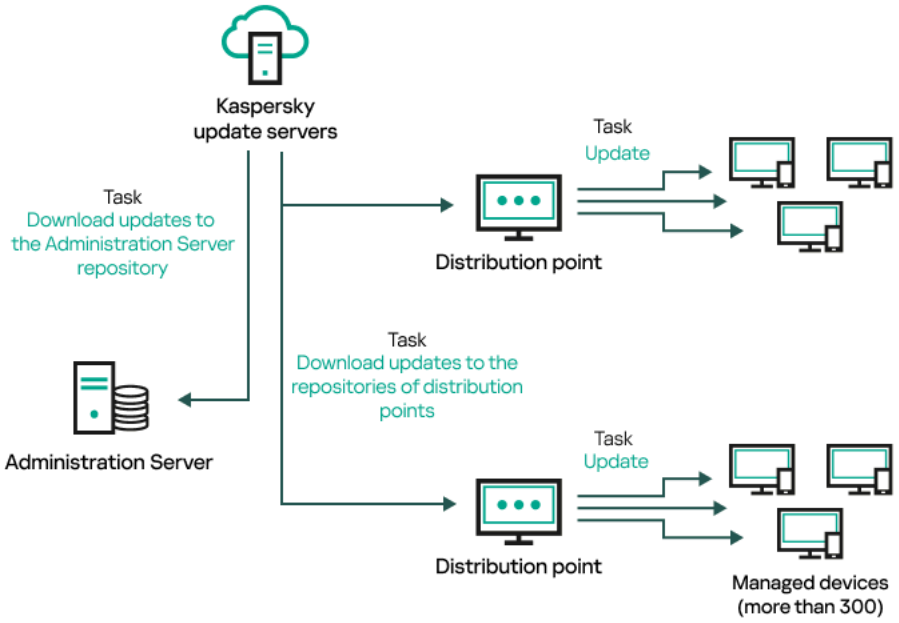
Каждое управляемое приложение "Лаборатории Касперского" запрашивает требуемые обновления с Сервера администрирования. Сервер администрирования объединяет эти запросы и загружает только те обновления, которые запрашиваются приложениями. Это обеспечивает то, что загружаются только нужные обновления и только один раз. При выполнении задачи *Загрузка обновлений в хранилище Сервера администрирования*, для обеспечения загрузки необходимых версий баз и модулей приложений "Лаборатории Касперского", на серверы обновлений "Лаборатории Касперского" автоматически, Сервер администрирования отправляет следующую информацию:

- идентификатор и версия приложения;
- идентификатор установки приложения;
- идентификатор активного ключа;
- идентификатор запуска задачи *Загрузка обновлений в хранилище Сервера администрирования*.

Передаваемая информация не содержит персональных данных и других конфиденциальных данных. АО "Лаборатория Касперского" защищает полученную информацию в соответствии с установленными законом требованиями.

Использование двух задач: Загрузка обновлений в хранилище Сервера администрирования и Загрузка обновлений в хранилища точек распространения

Вы можете загружать обновления в хранилища точек распространения непосредственно с серверов обновлений "Лаборатории Касперского" вместо хранилища Сервера администрирования, а затем распространять обновления на управляемые устройства (см. рисунок ниже). Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.



Обновление с использованием задачи Загрузка обновлений в хранилище Сервера администрирования и задачи Загрузка обновлений в хранилища точек распространения

По умолчанию Сервер администрирования и точки распространения взаимодействуют с серверами обновлений "Лаборатории Касперского" и загружают обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования и/или точки распространения на использование протокола HTTP вместо HTTPS.

Для реализации этой схемы создайте задачу *Загрузка обновлений в хранилища точек распространения* в дополнение к задаче *Загрузка обновлений в хранилище Сервера администрирования*. После этого точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

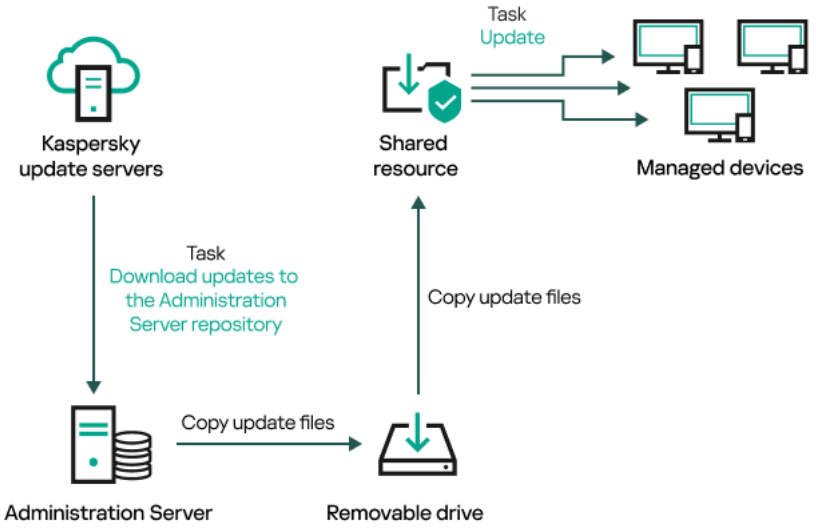
Точки распространения под управлением macOS не могут загружать обновления с серверов обновлений "Лаборатории Касперского".

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.

Для этой схемы также требуется задача *Загрузка обновлений в хранилище Сервера администрирования*, так как эта задача используется для загрузки баз и модулей приложений "Лаборатории Касперского" для Kaspersky Security Center.

Вручную через локальную папку, общую папку или FTP-сервер

Если клиентские устройства не подключены к Серверу администрирования, вы можете использовать локальную папку или общий ресурс в качестве источника обновления баз, модулей приложений и приложений "Лаборатории Касперского". В этой схеме вам нужно скопировать необходимые обновления из хранилища Сервера администрирования на съемный диск, а затем скопировать обновления в локальную папку или общий ресурс, указанный в качестве источника обновлений в параметрах Kaspersky Endpoint Security (см. рисунок ниже).



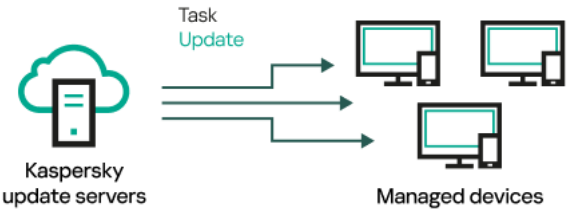
Обновление через локальную папку, общую папку или FTP-сервер

Подробнее об источниках обновлений в Kaspersky Endpoint Security см. в следующих справках:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux

Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security на управляемых устройствах

На управляемых устройствах вы можете настроить Kaspersky Endpoint Security на получение обновлений напрямую с серверов обновлений "Лаборатории Касперского" (см. рисунок ниже).



Обновление приложений безопасности непосредственно с серверов обновлений "Лаборатории Касперского"

В этой схеме приложения безопасности не используют хранилища, предоставленные Kaspersky Security Center. Чтобы получать обновления непосредственно с серверов обновлений "Лаборатории Касперского", укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений в интерфейсе программы безопасности. Дополнительные сведения об этих параметрах см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux

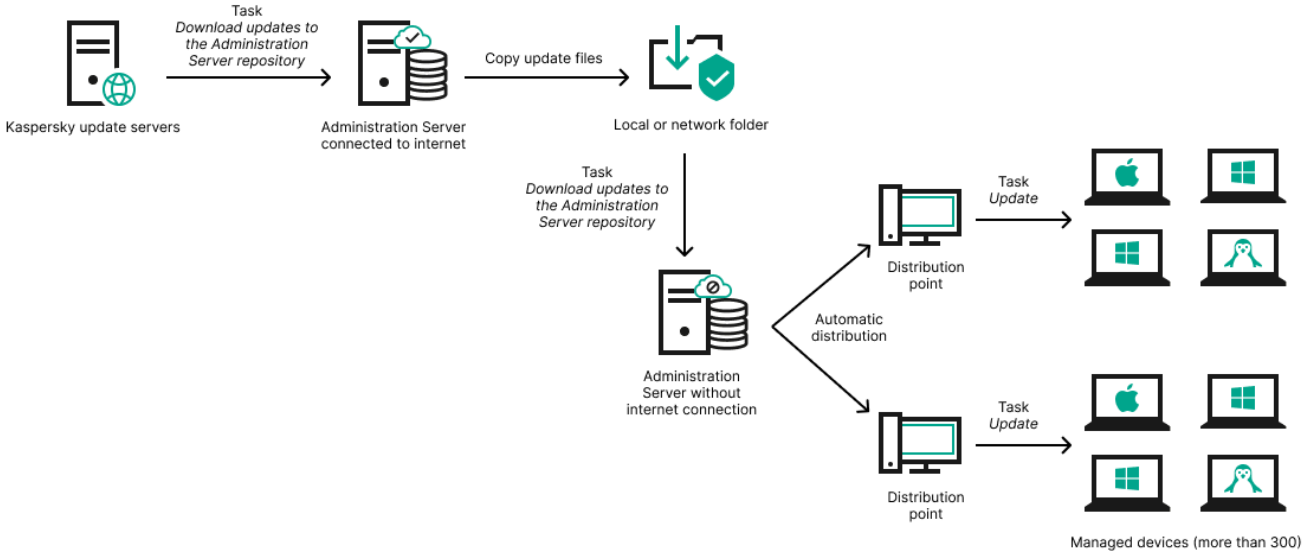
Через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

Если Сервер администрирования не имеет подключения к интернету, вы можете настроить задачу *Загрузка обновлений в хранилище Сервера администрирования* для загрузки обновлений из локальной или сетевой папки. В этом случае требуется время от времени копировать необходимые файлы обновлений в указанную папку. Например, вы можете скопировать необходимые файлы обновления из одного из следующих источников:

- Сервер администрирования, имеющий выход в интернет (см. рис. ниже).

  Так как Сервер администрирования загружает только те обновления, которые запрашиваются приложениями безопасности, наборы приложений безопасности, которыми управляют Серверы администрирования (подключенные и не подключенные к интернету) должны совпадать.

  Если Сервер администрирования, который вы используете для загрузки обновлений, имеет версию 13.2 или более раннюю, откройте свойства задачи *Загрузка обновлений в хранилище Сервера администрирования*, а затем включите параметр **Загружать обновления, используя старую схему**.



Обновление через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

- Kaspersky Update Utility

  Так как утилита использует старую схему для загрузки обновлений, откройте свойства задачи *Загрузка обновлений в хранилище Сервера администрирования*, а затем включите параметр **Загружать обновления, используя старую схему**.

Об использовании файлов различий для обновления баз и модулей приложений "Лаборатории Касперского"

Когда Kaspersky Security Center загружает обновления с серверов обновлений "Лаборатории Касперского", он оптимизирует трафик с помощью файлов различий. Вы также можете включить использование файлов различий устройствами (Серверов администрирования, точек распространения и клиентских устройств), которые принимают обновления с других устройств в вашей сети.

О функции загрузки файлов различий

Файл различий описывает различия между двумя версиями файлов базы или модулями приложения. Использование файлов различий сохраняет трафик внутри сети вашей организации, так как файлы различий занимают меньше места, чем целые файлы баз и модулей приложений. Если функция *Загрузить файлы различий* включена для Сервера администрирования или точки распространения, файлы различий сохраняются на этом Сервере администрирования или точке распространения. В результате устройства, которые получают обновления от этого Сервера администрирования или точки распространения, могут использовать сохраненные файлы различий для обновления своих баз и модулей приложений.

Для оптимизации использования файлов различий рекомендуется синхронизировать расписание обновления устройств с расписанием обновлений Сервера администрирования или точки распространения, с которых это устройство получает обновления. Однако трафик может быть сохранен, даже если устройства обновляются в несколько раз реже, чем Сервер администрирования или точки распространения, с которых устройство получает обновления.

Функция загрузки файлов различий может быть включена только на Серверах администрирования и точках распространения версии 11 и выше. Чтобы сохранить файлы различий на Серверах администрирования и точках распространения предыдущих версий, их необходимо обновить до версии 11 или выше.

Функция загрузки файлов различий несовместима с офлайн-моделью получения обновлений. Это означает, что Агенты администрирования, использующие офлайн-модель загрузки обновлений, не загружают файлы различий, даже если функция загрузки файлов различий включена на Сервере администрирования или точке распространения, которые предоставляют обновления этим Агентам администрирования.

Точки распространения не используют многоадресную IP-рассылку для автоматического распространения файлов различий.

Включение функции загрузки файлов различий

Предварительные требования

Необходимые предварительные условия для сценария:

- Сервер администрирования и точки распространения обновлены до версии 11 или выше.
- Офлайн модель получения обновлений выключена в свойствах политики Агента администрирования.

Этапы

1. **Включение функции на Сервере администрирования**

   Включите функцию в свойствах задачи Загрузка обновлений в хранилище Сервера администрирования.

2. **Включение функции для точки распространения**

   Включить функцию для точки распространения, которая получает обновления с помощью задачи Загрузка обновлений в хранилища точек распространения

   Включите функцию для точки распространения, которая получает обновления с Сервера администрирования.

   Эта функция включается в свойствах политики Агента администрирования и (если точки распространения назначены вручную и если вы хотите переопределить параметры политики) в свойствах Сервера администрирования в разделе **Точки распространения**.

Чтобы проверить, что функция загрузки файлов различий успешно включена, вы можете измерить внутренний трафик до и после выполнения сценария.

Создание задачи для загрузки обновлений в хранилище Сервера администрирования

Задача *Загрузка обновлений в хранилище Сервера администрирования* создается автоматически во время работы мастера первоначальной настройки Kaspersky Security Center. Задача *Загрузка обновлений в хранилище Сервера администрирования* может быть создана в одном экземпляре. Поэтому вы можете создать задачу *Загрузка обновлений в хранилище Сервера администрирования* только в случае, если она была удалена из списка задач Сервера администрирования.

Чтобы создать задачу загрузки обновлений в хранилище Сервера администрирования:

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания одним из следующих способов:
   - В контекстном меню **Задачи** в дереве консоли выберите пункт **Новый → Задачу**.
   - Нажмите на кнопку **Создать задачу** в рабочей области папки **Задачи**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. В окне мастера **Выбор типа задачи** выберите **Загрузка обновлений в хранилище Сервера администрирования**.
4. В окне мастера **Параметры**, укажите следующие параметры задачи:
   - **Источники обновлений**

     В качестве источника обновлений для Сервера администрирования 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 Сервер администрирования взаимодействует с серверами обновлений "Лаборатории Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.

Выбрано по умолчанию.

- Главный Сервер администрирования

  Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.

- Локальная или сетевая папка

  Локальная или сетевая папка, которая содержит последние обновления. Сетевая папка может быть FTP-сервером, HTTP-сервером или общим ресурсом SMB. 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".

- **Прочие параметры**:

  - **Принудительно обновить подчиненные Серверы**

    Если параметр включен, Сервер администрирования будет запускать задачи получения обновлений на подчиненных Серверах администрирования сразу после получения обновлений. Задачи обновления запускаются с использованием источника обновления, который настроен в свойствах задачи на подчиненных Серверах администрирования.

    Если этот параметр выключен, задачи обновления на подчиненных Серверах администрирования начинаются в соответствии с расписанием.

    По умолчанию параметр выключен.

  - **Копировать полученные обновления в дополнительные папки**

    Если флажок установлен, после получения обновлений Сервер администрирования будет копировать обновления в указанные папки. Используйте этот параметр, если хотите управлять вручную обновлениями на вашем устройстве.

    Например, вы можете использовать этот параметр в следующей ситуации: сеть организации содержит несколько независимых подсетей и устройства из каждой подсети не имеют доступ к другой подсети. При этом устройства во всех подсетях имеют доступ к общей сетевой папке. В этом случае для Сервера администрирования в одной из подсетей укажите загрузку обновлений с серверов обновлений "Лаборатории Касперского", включите этот параметр и укажите эту сетевую папку. В задаче загрузка обновлений в хранилище для Сервера администрирования укажите эту же сетевую папку в качестве источника обновлений.

    Если вы выберете копирование загруженных обновлений в локальную папку, необходимо указать на устройстве папку, которая содержит установленный Сервер администрирования. Путь к папке зависит от операционной системы устройства. Поскольку локальная папка расположена на Сервере администрирования с операционной системой Linux, вам нужно указать POSIX-путь, например, /path/to/dir.

При выборе сетевой папки, расположенной на Сервере администрирования с операционной системой Linux, нужно заранее обеспечить доступ к сетевой папке с устройства, на котором установлен Сервер администрирования, смонтировав папку. Доступ к папке осуществляется с использованием SMB-протокола.

По умолчанию параметр выключен.

- **Не обновлять устройства и подчиненные Серверы администрирования принудительно до окончания копирования**

  Если флажок установлен, задачи получения обновлений клиентскими устройствами и подчиненными Серверами администрирования будут запускаться после окончания копирования обновлений из сетевой папки обновлений в дополнительные папки обновлений.

  Этот флажок должен быть установлен, если клиентские устройства и подчиненные Серверы администрирования скачивают обновления из дополнительных сетевых папок.

  По умолчанию параметр выключен.

- **Загружать обновления, используя старую схему**

  Начиная с версии 14, Kaspersky Security Center загружает обновления баз и модулей приложений по новой схеме. Чтобы приложение могло загружать обновления с помощью новой схемы, источник обновлений должен содержать файлы обновлений с метаданными, совместимыми с новой схемой. Если источник обновлений содержит файлы обновлений с метаданными, совместимыми только со старой схемой, включите параметр **Загружать обновления, используя старую схему**. Иначе задача загрузки обновлений завершится ошибкой.

  Например, этот параметр необходимо включить, если в качестве источника обновлений указана локальная или сетевая папка, а файлы обновлений в эту папку были загружены одним из следующих приложений:

  - Kaspersky Update Utility

    Эта утилита загружает обновления по старой схеме.

  - Kaspersky Security Center

    Например, один Сервер администрирования не имеет подключения к интернету. В этом случае можно загружать обновления с помощью второго Сервера администрирования, подключенного к интернету, а затем помещать обновления в локальную или сетевую папку, чтобы использовать ее в качестве источника обновлений для первого Сервера. Если второй Сервер администрирования имеет номер версии 13.2 или ниже, включите параметр **Загружать обновления, используя старую схему** в задаче для первого Сервера администрирования.

  По умолчанию параметр выключен.

5. На странице **Настройка расписания запуска задачи** мастера можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

   - **Запуск по расписанию:**

     Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

     - **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.

- **Каждые N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживается переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

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

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

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

  По умолчанию выбран этот вариант.

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

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

По умолчанию 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 случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

6. На странице **Определение названия задачи** мастера укажите название создаваемой задачи. Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

7. На странице **Завершение создания задачи** мастера нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

После завершения работы мастера созданная задача **Загрузка обновлений в хранилище Сервера администрирования** появится в рабочей области списка задач Сервера администрирования.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

В результате выполнения задачи *Загрузка обновлений в хранилище Сервера администрирования* обновления баз и модулей приложений копируются с источника обновлений и размещаются в папке общего доступа. Если задача создается для группы администрирования, то она распространяется только на Агенты администрирования, входящие в указанную группу администрирования.

Из папки общего доступа обновления распространяются на клиентские устройства и подчиненные Серверы администрирования.

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.

Вы можете использовать эту задачу, например, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет. Если точка распространения подключается к интернету с помощью прокси-сервера, вам нужно указать соответствующие параметры политики Агента администрирования.

Чтобы создать задачу загрузки обновлений в хранилища точек распространения для выбранной группы администрирования:

1. В дереве консоли выберите папку **Задачи**.
2. По кнопке **Новая задача** в рабочей области папки запустите мастер создания задачи.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. В окне **Выбор типа задачи** мастера создания задачи выберите узел **Сервер администрирования Kaspersky Security Center**, раскройте папку **Дополнительно** и выберите задачу **Загрузка обновлений в хранилища точек распространения**.
4. В окне мастера **Параметры**, укажите следующие параметры задачи:

   - **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.

- **Загружать обновления, используя старую схему**

  Начиная с версии 14, Kaspersky Security Center загружает обновления баз и модулей приложений по новой схеме. Чтобы приложение могло загружать обновления с помощью новой схемы, источник обновлений должен содержать файлы обновлений с метаданными, совместимыми с новой схемой. Если источник обновлений содержит файлы обновлений с метаданными, совместимыми только со старой схемой, включите параметр **Загружать обновления, используя старую схему**. Иначе задача загрузки обновлений завершится ошибкой.

  Например, этот параметр необходимо включить, если в качестве источника обновлений указана локальная или сетевая папка и файлы обновлений в этой папке были загружены одной из следующих приложений:

  - Kaspersky Update Utility

    Эта утилита загружает обновления по старой схеме.

  - Kaspersky Security Center

    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 **Загружать обновления, используя старую схему** в задаче *Загружать обновления в хранилища точек распространения*.

  По умолчанию параметр выключен.

5. В окне мастера **Выберите группу администрирования** нажмите на кнопку **Обзор** и выберите группу администрирования, для которой задача будет применена.

6. На странице **Настройка расписания запуска задачи** мастера можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

   - **Запуск по расписанию:**

     Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

     - **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.

- **Каждые N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживается переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

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

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

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

  По умолчанию выбран этот вариант.

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

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

  По умолчанию 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 случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

7. На странице **Определение названия задачи** мастера укажите название создаваемой задачи. Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

8. На странице **Завершение создания задачи** мастера нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

После завершения работы мастера созданная задача **Загрузка обновлений в хранилища точек распространения** появится в списке задач Агента администрирования в соответствующей группе администрирования и в папке **Задачи**.

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.

В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Точки распространения**. В свойствах каждой точки распространения в разделе **Источник обновлений** можно указать источник обновлений (**Получать с Сервера администрирования** или **Использовать задачу принудительной загрузки обновлений**). Для точки распространения, назначенной вручную или автоматически, по умолчанию выбран вариант **Получать с Сервера администрирования**. Такие точки распространения будут использовать результаты задачи *Загрузка обновлений в хранилища точек распространения*.

В свойствах каждой точки распространения указана сетевая папка, настроенная индивидуально для этой точки распространения. Названия папок могут быть разными для разных точек распространения. Поэтому не рекомендуется изменять сетевую папку обновлений в свойствах задачи, если задача создается для группы устройств.

Вы можете изменить сетевую папку обновлений в свойствах задачи *Загрузка обновлений в хранилища точек распространения*, если вы создаете локальную задачу для устройства.

Настройка параметров задачи загрузки обновлений в хранилище Сервера администрирования

Чтобы настроить параметры задачи загрузки обновлений в хранилище Сервера администрирования:

1. В рабочей области папки дерева консоли **Задачи** выберите задачу **Загрузка обновлений в хранилище Сервера администрирования** в списке задач.

2. Откройте окно свойств задачи одним из следующих способов:

   - В контекстном меню файла выберите пункт **Свойства**.

   - По ссылке **Настроить параметры задачи** в блоке работы с выбранной задачей.

   Откроется окно свойств задачи *Загрузка обновлений в хранилище Сервера администрирования*. В нем вы можете настроить параметры загрузки обновлений в хранилище Сервера администрирования.

Проверка полученных обновлений

Перед установкой обновлений на управляемые устройства вы можете сначала проверить их на работоспособность и ошибки с помощью задачи *Проверка обновлений*. Задача *Проверка обновлений* выполняется автоматически в рамках задачи *Загрузка обновлений в хранилище Сервера администрирования*. Сервер администрирования загружает обновления с источника, сохраняет их во временном хранилище и запускает задачу *Проверка обновлений*. В случае успешного выполнения этой задачи обновления копируются из временного хранилища в папку общего доступа Сервера администрирования (<Папка установки Kaspersky Security Center>\Share\Updates). Обновления распространяются на клиентские устройства, для которых Сервер администрирования является источником обновления.

Если по результатам выполнения задачи *Проверка обновлений* размещенные во временном хранилище обновления признаны некорректными или задача *Проверка обновлений* завершается с ошибкой, копирование обновлений в папку общего доступа не производится. На Сервере администрирования остается предыдущий набор обновлений. Запуск задач с типом расписания **При загрузке обновлений в хранилище** также не выполняется. Эти операции выполняются при следующем запуске задачи *Загрузка обновлений в хранилище Сервера администрирования*, если проверка нового набора обновлений завершится успешно.

Набор обновлений считается некорректным, если хотя бы на одном из тестовых устройств выполняется одно из следующих условий:

- произошла ошибка выполнения задачи обновления;

- после применения обновлений изменился статус постоянной защиты приложения безопасности;

- в ходе выполнения задачи проверки по требованию был найден зараженный объект;

- произошла ошибка функционирования приложения "Лаборатории Касперского".

Если ни одно из перечисленных условий ни на одном из тестовых устройств не выполняется, набор обновлений признается корректным и задача *Проверка обновлений* считается успешно выполненной.

Прежде чем приступить к созданию задачи *Проверка обновлений*, выполните предварительные условия:

1. Создайте группу администрирования с несколькими тестовыми устройствами. Эта группа понадобится вам для проверки обновлений.

   В качестве тестовых устройств рекомендуется использовать хорошо защищенные устройства с наиболее распространенной в сети организации программной конфигурацией. Такой подход повышает качество и вероятность обнаружения вирусов при проверке, а также минимизирует риск ложных срабатываний. При нахождении вирусов на тестовых устройствах задача *Проверка обновлений* считается завершившейся неудачно.

2. Создайте задачи *Обновление* и *Поиск вредоносного ПО* для приложения, поддерживаемого Kaspersky Security Center, например, Kaspersky Endpoint Security для Windows или Kaspersky Security для Windows Server. При создании задач *Обновление* и *Поиск вредоносного ПО* укажите группу администрирования с тестовыми устройствами.

   Задача *Проверка обновлений* последовательно запускает задачи *Обновление* и *Поиск вредоносного ПО* на тестовых устройствах и так проверяет, что все обновления актуальны. Также при создании задачи *Проверка обновлений* необходимо указать задачи *Обновление* и *Поиск вредоносного ПО*.

3. Создайте задачу *Загрузка обновлений в хранилище Сервера администрирования*.

Чтобы Kaspersky Security Center проверял полученные обновления перед распространением их на клиентские устройства:

1. В рабочей области папки **Задачи** дерева консоли выберите задачу *Загрузка обновлений в хранилище Сервера администрирования* в списке задач.

2. Откройте окно свойств задачи одним из следующих способов:

   - В контекстном меню файла выберите пункт **Свойства**.

   - По ссылке **Настроить параметры задачи** в блоке работы с выбранной задачей.

3. Если задача *Проверка обновлений* существует, нажмите на кнопку **Обзор**. В открывшемся окне выберите задачу *Проверка обновлений* в группе администрирования с тестовыми устройствами.

4. Если вы не создали задачу *Проверка обновлений* ранее, нажмите на кнопку **Создать**.

   Запустится мастер создания задачи *Проверка обновлений*. Следуйте далее указаниям мастера.

5. Закройте окно свойств задачи *Загрузка обновлений в хранилище Сервера администрирования*, нажав на кнопку **OK**.

Автоматическая проверка обновлений включена. Теперь вы можете запустить задачу *Загрузка обновлений в хранилище Сервера администрирования*, и она начнется с проверки обновлений.

Настройка проверочных политик и вспомогательных задач

При создании задачи *Проверка обновлений* Сервер администрирования формирует проверочные политики, а также вспомогательные групповые задачи обновления и проверки по требованию.

Обновления вспомогательных групп и задачи проверки по требованию занимают некоторое время. Эти задачи выполняются при выполнении задачи *Проверка обновлений*. Задача *Проверка обновлений* выполняется в рамках выполнения задачи *Загрузка обновлений в хранилище*. Время выполнения задачи *Загрузки обновлений в хранилище* включает в себя время выполнения вспомогательных групповых задач обновления и проверки по требованию.

Вы можете изменить параметры тестовых политик и вспомогательных задач.

Чтобы изменить параметры проверочной политики или вспомогательной задачи:

1. В дереве консоли выберите группу, для которой сформирована задача *Проверка обновлений*.
2. В рабочей области группы выберите одну из следующих вкладок:
   - **Политики**, если вы хотите изменить параметры проверочной политики.
   - **Задачи**, если вы хотите изменить параметры вспомогательной задачи.
3. В рабочей области вкладки выберите политику или задачу, параметры которой вы хотите изменить.
4. Откройте окно свойств этой политики (задачи) одним из следующих способов:
   - В контекстном меню политики (задачи) выберите пункт **Свойства**.
   - По ссылке **Настроить параметры политики** (**Настроить параметры задачи**) в блоке работы с выбранной политикой (задачей).

Чтобы проверка обновлений выполнялась правильно, необходимо соблюдать следующие ограничения на изменение параметров проверочных политик и вспомогательных задач:

- В параметрах вспомогательных задач:
  - Сохранять на Сервере администрирования все события с уровнями важности **Критическое событие** и **Отказ функционирования**. На основе событий этих типов Сервер администрирования проводит анализ работы приложений.
  - Используйте Сервер администрирования как источник обновлений.
  - Укажите тип расписания задачи – **Вручную**.

- В параметрах проверочных политик:
  - Отключить технологии проверки iChecker и iSwift (**Базовая защита → Защита от файловых угроз → Параметры → Дополнительно → Технологии проверки**).
  - Выберите действия с зараженными объектами: **Лечить; удалить, если лечение не удалось** / **Лечить; заблокировать, если лечение не удалось** / **Блокировать**. (**Базовая защита → Защита от файловых угроз → Действия при обнаружении угрозы**).
- В параметрах тестовых политик и вспомогательных задач:

  Если после установки обновлений модулей приложений потребуется перезагрузка устройства, ее следует выполнить незамедлительно. Если устройство не будет перезагружено, то проверить этот тип обновлений будет невозможно. Для некоторых приложений установка обновлений, требующих перезагрузки, может быть запрещена или выполняться только после подтверждения от пользователя. Эти ограничения должны быть отключены в параметрах проверочных политик и вспомогательных задач.

Просмотр полученных обновлений

Чтобы просмотреть список полученных обновлений,

В дереве консоли в папке **Хранилища** выберите вложенную папку **Обновления баз и модулей приложений "Лаборатории Касперского"**.

В рабочей области папки **Обновления баз и модулей приложений "Лаборатории Касперского"** представлен список обновлений, сохраненных на Сервере администрирования.

Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства

Вы можете настроить автоматическое обновление баз и модулей приложения Kaspersky Endpoint Security на клиентских устройствах.

Чтобы настроить загрузку и автоматическую установку обновлений Kaspersky Endpoint Security на устройства:

1. В дереве консоли выберите папку **Задачи**.
2. Создайте задачу с типом **Обновление** одним из следующих способов:
   - В контекстном меню папки дерева консоли **Задачу** выберите пункт **Создать → Задачи**.
   - В рабочей области папки **Новая задача** нажмите на кнопку **Задачи**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. В окне мастера **Выбор типа задачи** выберите тип задачи **Kaspersky Endpoint Security**, затем подтип задачи **Обновление**.

4. Следуйте дальнейшим шагам мастера.

   В результате работы мастера создается задача обновления для Kaspersky Endpoint Security. Созданная задача отображается в списке задач в рабочей области папки **Задачи**.

5. В рабочей области папки **Задачи** выберите созданную задачу обновления.

6. В контекстном меню задачи выберите пункт **Свойства**.

7. В открывшемся окне свойств задачи в панели **Разделы** выберите раздел **Свойства**.

   В разделе **Свойства** можно настроить параметры задачи обновления в локальном и мобильном режимах:

   - **Параметры обновления в локальном режиме**: между устройством и Сервером администрирования установлена связь.
   - **Обновите параметры для автономного режима**: между устройством и Kaspersky Security Center не установлена связь (например, если устройство не подключено к интернету).

8. По кнопке **Параметры** выберите источник обновлений.

9. Выберите параметр **Загружать обновления модулей приложения**, чтобы одновременно с базами приложения загружать и устанавливать обновления модулей приложения.

   Если флажок установлен, то Kaspersky Endpoint Security уведомляет пользователя о доступных обновлениях модулей приложения и во время выполнения задачи обновления включает обновления модулей приложения в пакет обновлений. Настройте применение модулей обновлений:

   - **Устанавливать критические и одобренные обновления**. При наличии обновлений модулей приложения Kaspersky Endpoint Security устанавливает обновления со статусом *Предельный* автоматически; остальные обновления модулей приложения – после одобрения их установки администратором.
   - **Устанавливать только утвержденные обновления**. При наличии обновлений модулей приложения Kaspersky Endpoint Security устанавливает их после одобрения их установки, локально через интерфейс приложения или с помощью Kaspersky Security Center.

   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.

10. Выберите параметр **Копировать обновления в папку**, чтобы приложение сохраняло загруженные обновления в папку, указанную по кнопке **Обзор**.

11. Нажмите на кнопку **ОК**.

При выполнении задачи **Обновление** приложение отправляет запросы серверам обновлений "Лаборатории Касперского".

Некоторые обновления требуют установки последних версий плагинов управляемых приложений.

Офлайн-модель получения обновлений

Агент администрирования на управляемых устройствах не всегда может подключиться к Серверу администрирования для получения обновлений. Например, Агент администрирования может быть установлен на ноутбук, который иногда не подключен к интернету и локальной сети. Также администратор может ограничить время подключения устройств к сети. В таких случаях устройства с установленным Агентом администрирования не смогут получить обновления от Сервера администрирования в соответствии с расписанием. Если настроено обновление управляемых приложений (например, Kaspersky Endpoint Security) с помощью Агента администрирования, для обновления требуется соединение с Сервером администрирования. Когда соединение между Агентом администрирования и Сервером администрирования отсутствует, обновление невозможно. Соединение Агента администрирования с Сервером может быть настроено так, чтобы Агент подключался к Серверу только в определенные периоды времени. В худшем случае, если настроенные периоды подключения "пересекаются" с периодами, когда связь отсутствует, базы никогда не будут обновлены. Также возможны ситуации, когда много управляемых приложений одновременно обращаются к Серверу администрирования за обновлениями. В этом случае Сервер администрирования может перестать отвечать на запросы (как во время DDoS-атаки).

Во избежание описанных проблем в Kaspersky Security Center реализована офлайн-модель получения обновления баз и модулей управляемых приложений. Эта модель обеспечивает механизм распространения обновлений вне зависимости от временных проблем, вызванных недоступностью каналов связи Сервера администрирования. Эта модель также снижает нагрузку на Сервер администрирования.

Как работает офлайн-модель получения обновлений

Когда Сервер администрирования получает обновления, он уведомляет Агент администрирования (на устройствах, где он установлен) об обновлениях, которые потребуются для управляемых приложений. Когда Агенты администрирования получают информацию об обновлениях, они загружают нужные файлы с Сервера администрирования заранее. При первом соединении с Агентом администрирования Сервер инициирует загрузку обновлений этим Агентом. После того как Агент администрирования на клиентском устройстве загрузит все обновления, обновления становятся доступными для приложений на устройстве.

Когда управляемое приложение на клиентском устройстве обращается к Агенту администрирования за обновлениями, Агент проверяет, есть ли у него необходимые обновления. Если обновления были получены от Сервера администрирования не раньше, чем за 25 часов с момента запроса управляемого приложения, Агент администрирования не подключается к Серверу администрирования и предоставляет управляемому приложению обновления из локального кеша. Соединение с Сервером администрирования может не выполняться, когда Агент администрирования предоставляет обновления для приложений на клиентских устройствах, но подключение не требуется для обновления.

Чтобы распределить нагрузку на Сервер администрирования, Агент администрирования на устройстве подключается к Серверу и загружает обновления случайным образом в течение интервала времени, определенного Сервером. Интервал времени зависит от количества устройств с установленным Агентом администрирования, которые загружают обновления, и от размера обновлений. Для снижения нагрузки на Сервер администрирования вы можете использовать Агент администрирования в качестве точки распространения.

Если офлайн-модель получения обновлений отключена, обновления распространяются в соответствии с расписанием задачи загрузки обновлений в хранилище.

По умолчанию офлайн-модель получения обновлений включена.

Офлайн-модель получения обновлений используется только для тех управляемых устройств, на которых задача получения обновлений управляемыми приложениями имеет расписание **При загрузке обновлений в хранилище**. Для остальных управляемых устройств используется традиционная система получения обновлений с Сервера администрирования в реальном времени.

Рекомендуется выключить офлайн-модель получения обновлений через настройки политик Агента администрирования соответствующих групп администрирования, если в управляемых приложениях настроено получение обновлений не с Сервера администрирования, а с серверов "Лаборатории Касперского" либо из сетевой папки и при этом задача получения обновлений имеет расписание **При загрузке обновлений в хранилище**.

Включение и выключение офлайн-модели получения обновлений

Не рекомендуется выключать офлайн-модель получения обновлений. Выключение может привести к сбоям в доставке обновлений на устройства. В некоторых случаях специалисты Службы технической поддержки "Лаборатории Касперского" могут рекомендовать вам снять флажок **Загружать обновления и антивирусные базы с Сервера администрирования заранее**. Тогда вам нужно будет убедиться, что задача загрузки обновлений в хранилище для приложений "Лаборатории Касперского" настроена.

Чтобы включить или выключить офлайн-модель получения обновлений для группы администрирования:

1. В дереве консоли выберите группу администрирования, для которой требуется включить офлайн-модель получения обновлений.
2. В рабочей области группы откройте вкладку **Политики**.
3. На вкладке **Политики** выберите политику Агента администрирования.
4. В контекстном меню политики выберите пункт **Свойства**.

   Откроется окно свойств политики Агента администрирования.
5. В окне свойств политики выберите раздел **Управление патчами и обновлениями**.
6. Установите или снимите флажок **Загружать обновления и антивирусные базы с Сервера администрирования заранее (рекомендуется)**, чтобы включить или выключить офлайн-модель получения обновлений соответственно.

   По умолчанию офлайн-модель получения обновлений включена.

В результате офлайн-модель получения обновлений будет включена или выключена.

Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center

По умолчанию автоматически устанавливаются загруженные обновления и патчи для следующих компонентов приложения:

- Агент администрирования для Windows
- Консоль администрирования
- Сервер iOS MDM

Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center доступна только для устройств под управлением Windows. Вы можете выключить автоматическую установку обновлений и патчей для этих компонентов. В этом случае 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.

Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center

Автоматическая установка обновлений для компонентов Kaspersky Security Center 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 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. Вы можете включить автоматическую установку позже с помощью политики.

Чтобы выключить автоматическую установку обновлений для компонентов Kaspersky Security Center при установке Агента администрирования на устройство с помощью инсталляционного пакета:

1. В дереве консоли выберите папку **Удаленная установка → Инсталляционные пакеты**.
2. В контекстном меню пакета **Агент администрирования Kaspersky Security Center <номер версии>** выберите пункт **Свойства**.
3. В свойствах инсталляционного пакета, в разделе **Параметры** снимите флажок **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. Вы можете включить автоматическую установку позже с помощью политики.

Если при установке Агента администрирования на устройство флажок был установлен (снят), 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 с помощью политики Агента администрирования:

1. В дереве консоли выберите группу администрирования, для которой требуется включить или выключить автоматическую установку обновлений и патчей.
2. В рабочей области группы откройте вкладку **Политики**.
3. На вкладке **Политики** выберите политику Агента администрирования.
4. В контекстном меню политики выберите пункт **Свойства**.

   Откроется окно свойств политики Агента администрирования.
5. В окне свойств политики выберите раздел **Управление патчами и обновлениями**.
6. Установите или снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**, чтобы включить или выключить автоматическую установку обновлений и патчей.
7. Установите замок при этом флажке.

Политика применится к выбранным устройствам, и автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center будет включена (выключена) на этих устройствах.

Автоматическое распространение обновлений

Kaspersky Security Center позволяет автоматически распространять и устанавливать обновления на клиентские устройства и подчиненные Серверы администрирования.

Автоматическое распространение обновлений на клиентские устройства

Чтобы обновления выбранного вами приложения автоматически распространялись на клиентские устройства сразу после загрузки обновлений в хранилище Сервера администрирования:

1. Подключитесь к Серверу администрирования, под управлением которого находятся клиентские устройства.

2. Создайте задачу распространения обновлений этого приложения для выбранных клиентских устройств одним из следующих способов:

   - Если требуется распространять обновления на клиентские устройства, входящие в выбранную группу администрирования, создайте задачу для выбранной группы.

   - Если требуется распространять обновления на клиентские устройства, входящие в разные группы администрирования или не входящие в группы администрирования, создайте задачу для набора устройств.

   Запустится мастер создания задачи. Следуйте его указаниям, выполнив следующие условия:

   a. В окне мастера **Тип задачи** в узле нужного вам приложения выберите задачу распространения обновлений.

      Название задачи распространения обновлений, которое отображается в окне **Тип задачи**, зависит от приложения, для которого создается задача. Подробнее о названиях задач обновления для выбранных приложений "Лаборатории Касперского" см. в руководствах к этим приложениям.

   b. В окне мастера **Расписание** в поле **Запуск по расписанию** выберите вариант запуска **При загрузке обновлений в хранилище**.

   В результате созданная задача распространения обновлений будет запускаться для выбранных устройств каждый раз при загрузке обновлений в хранилище Сервера администрирования.

Если задача распространения обновлений нужного вам приложения уже создана для выбранных устройств, для автоматического распространения обновлений на клиентские устройства в окне свойств задачи в разделе **Расписание** нужно выбрать вариант запуска **При загрузке обновлений в хранилище** в поле **Запуск по расписанию**.

Автоматическое распространение обновлений на подчиненные Серверы администрирования

Чтобы обновления выбранного вами приложения автоматически распространялись на подчиненные Серверы администрирования сразу после загрузки обновлений в хранилище главного Сервера администрирования:

1. В дереве консоли в узле главного Сервера администрирования выберите папку **Задачи**.
2. В списке задач в рабочей области выберите задачу загрузки обновлений в хранилище Сервера администрирования.
3. Откройте раздел **Параметры** окна свойств выбранной задачи одним из следующих способов:
   - В контекстном меню файла выберите пункт **Свойства**.
   - По ссылке **Изменить параметры** в блоке работы с выбранной задачей.
4. В разделе **Параметры** окна свойств задачи откройте окно **Прочие параметры** по ссылке **Настроить** в подразделе Прочие параметры.
5. В открывшемся окне **Прочие параметры** установите флажок **Принудительно обновить подчиненные Серверы**.
6. В параметрах задачи получения обновлений Сервером администрирования на вкладке **Параметры** окна свойств задачи установите флажок **Принудительно обновить подчиненные Серверы**.

После получения обновлений главным Сервером администрирования будут автоматически запускаться задачи загрузки обновлений подчиненными Серверами администрирования, независимо от расписания, установленного в параметрах этих задач.

Главный Сервер администрирования обновляет антивирусные базы в соответствии с приложениями, установленными на подчиненных Серверах администрирования. Установка дополнительных плагинов и создание инсталляционных пакетов на главном Сервере администрирования не требуется.

Автоматическое назначение точек распространения

Рекомендуется назначать точки распространения автоматически. Kaspersky Security Center будет сам выбирать, какие устройства назначать точками распространения.

Чтобы назначить точки распространения автоматически:

1. Откройте главное окно приложения.
2. В дереве консоли выберите узел с именем Сервера администрирования, для которого требуется автоматически назначать точки распространения.
3. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
4. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Точки распространения**.

5. В правой части окна выберите параметр **Автоматически назначать точки распространения**.

> Если автоматическое назначение устройств точками распространения включено, невозможно вручную настраивать параметры точек распространения, а также изменять список точек распространения.

6. Нажмите на кнопку **OK**.

В результате Сервер администрирования будет автоматически назначать точки распространения и настраивать их параметры.

Назначение устройства точкой распространения вручную

Kaspersky Security Center позволяет назначать устройства точками распространения.

Рекомендуется назначать точки распространения автоматически. В этом случае Kaspersky Security Center будет сам выбирать, какие устройства назначать точками распространения. Однако если вы по какой-то причине хотите отказаться от автоматического назначения точек распространения (например, если вы хотите использовать специально выделенные серверы), вы можете назначать точки распространения вручную, предварительно рассчитав их количество и конфигурацию.

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 дереве консоли выберите узел **Сервер администрирования**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Точки распространения** нажмите на кнопку **Добавить**. Кнопка доступна, если выбран вариант **Вручную назначать точки распространения**.

   Откроется окно **Добавление точки распространения**.
4. В окне **Добавление точки распространения** выполните следующие действия:

   a. Выберите устройство, которое будет выполнять роль точки распространения (в группе администрирования или укажите IP-адрес устройства). При выборе устройства учитывайте особенности работы точек распространения и требования к устройству, которое выполняет роль точки распространения.

   b. Укажите набор устройств, на которые точка распространения будет распространять обновления. Вы можете указать группу администрирования или описание сетевого местоположения.
5. Нажмите на кнопку **OK**.

   Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.
6. Выберите в списке добавленную точку распространения и по кнопке **Свойства** откройте окно ее свойств.

7. В окне свойств настройте параметры точки распространения:

- В разделе **Общие** укажите параметры взаимодействия точки распространения с клиентскими устройствами.

  - **SSL-порт**

    Номер SSL-порта, по которому осуществляется защищенное подключение клиентских устройств к точке распространения с использованием протокола SSL.

    По умолчанию номер порта – 13000.

  - **Использовать многоадресную IP-рассылку**

    Если параметр включен, для автоматического распространения инсталляционных пакетов на клиентские устройства в пределах группы будет использоваться многоадресная IP-рассылка.

    Многоадресная IP-рассылка уменьшает время, необходимое для установки приложений из инсталляционного пакета на группу клиентских устройств, но увеличивает время установки при установке приложения на одно клиентское устройство.

  - **Адрес IP-рассылки**

    IP-адрес, на который будет выполняться многоадресная рассылка. IP-адрес можно задать в диапазоне 224.0.0.0 – 239.255.255.255

    По умолчанию Kaspersky Security Center автоматически назначает уникальный IP-адрес многоадресной рассылки в заданном диапазоне.

  - **Номер порта IP-рассылки**

    Номер порта многоадресной рассылки.

    Номер порта по умолчанию – 15001. Если в качестве точки распространения указано устройство, на котором установлен Сервер администрирования, то для подключения с использованием SSL-протокола по умолчанию используется порт 13001.

  - **Распространять обновления**

    Обновления распространяются на управляемые устройства из следующих источников:

    - Эта точка распространения, если этот параметр включен.
    - Другие точки распространения, Сервер администрирования или серверы обновлений "Лаборатории Касперского", если параметр выключен.

    Если вы используете точки распространения для распространения обновлений, вы можете сэкономить трафик, так как уменьшите количество загрузок. Также вы можете снизить нагрузку на Сервер администрирования и перераспределить нагрузку между точками распространения. Вы можете вычислить количество точек распространения в вашей сети для оптимизации трафика и нагрузки.

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

- **Распространять инсталляционные пакеты**

  Инсталляционные пакеты распространяются на управляемые устройства из следующих источников:

  - Эта точка распространения, если этот параметр включен.
  - Другие точки распространения, Сервер администрирования или серверы обновлений "Лаборатории Касперского", если параметр выключен.

  Если вы используете точки распространения для распространения инсталляционных пакетов, вы можете сэкономить трафик, так как уменьшите количество загрузок. Также вы можете снизить нагрузку на Сервер администрирования и перераспределить нагрузку между точками распространения. Вы можете вычислить количество точек распространения в вашей сети для оптимизации трафика и нагрузки.

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

- **Использовать точку распространения в качестве извещающего сервера**

  В Kaspersky Security Center точка распространения может работать как push-сервер для устройств, которые управляются по мобильному протоколу. Например, push-сервер должен быть включен, если вы хотите включить принудительную синхронизацию устройств с KasperskyOS с Сервером администрирования. Push-сервер имеет ту же область управляемых устройств, что и точка распространения, на которой включен push-сервер. Если у вас есть несколько точек распространения, назначенных для одной и той же группы администрирования, вы можете включить извещающий сервер на каждой них. В этом случае Сервер администрирования распределяет нагрузку между точками распространения.

  Если вы управляете устройствами с установленной операционной системой KasperskyOS или планируете это сделать, вам нужно использовать точку распространения в качестве push-сервера. Вы также можете использовать точку распространения в качестве push-сервера, если хотите отправлять push-уведомления на клиентские устройства.

- **Порт push-сервера**

  Порт точки распространения, который клиентские устройства будут использовать для подключения. По умолчанию номер порта – 13295.

- В разделе **Область действия** укажите область, на которую точка распространения распространяет обновления (группы администрирования и/или сетевое местоположение).

- В разделе **Прокси-сервер KSN** вы можете настроить приложение так, чтобы точка распространения использовалась для пересылки KSN запросов от управляемых устройств.

  - **Включить прокси-сервер KSN на стороне точки распространения**

    Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

    Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского".

    По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены в окне свойств Сервера администрирования.

    Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

- **Переслать KSN запрос Серверу администрирования**

  Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

  По умолчанию параметр включен.

- **Доступ к облачной службе KSN/KPSN непосредственно через интернет**

  Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или KPSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или KPSN.

  Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к KPSN. Если вы хотите перенастроить точки распространения для отправки запросов KSN в KPSN, включите параметр **Пересылать KSN запрос Серверу администрирования** для каждой точки распространения.

  Точки распространения с установленным Агентом администрирования версии 12 (и выше) могут напрямую обращаться к KPSN.

- **Игнорировать параметры прокси-сервера для подключения к KPSN**

  Установите этот флажок, если параметры прокси-сервера настроены в свойствах точки распространения или политики Агента администрирования, но ваша архитектура сети требует, чтобы вы использовали KPSN напрямую. В противном случае запрос от управляемого приложения не будет передан в KPSN.

  Это параметр доступен, если вы выбрали параметр **Доступ к облачной службе KSN/KPSN непосредственно через интернет**.

- **TCP-порт**

  Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.

- **UDP-порт**

  Чтобы Агент администрирования подключался к Серверу администрирования через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **Номер UDP-порт** укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к Серверу администрирования выполняется через UDP-порт 15000.

- **HTTPS-порт**

  Если вам нужно, чтобы управляемые устройства подключались к прокси-серверу KSN через порт HTTPS, включите параметр **Использовать HTTPS** и укажите номер порта в поле **Через HTTPS-порт**. По умолчанию подключение к прокси-серверу KSN выполняется через HTTPS-порт 17111.

- В разделе **Обнаружение устройств** настройте опрос доменов Windows, Active Directory и IP-диапазонов точкой распространения.

  - **Windows-домены**

    Вы можете включить обнаружение устройств для Windows-доменов и задать его расписание.

  - **Active Directory**

    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.

- **IP-диапазоны**

  Вы можете включить обнаружение устройств для IPv4-диапазонов и IPv6-сетей.

  Если вы включили параметр **Разрешить опрос диапазона**, вы можете добавить диапазон опроса и задать расписание опроса. Вы можете добавить IP-диапазоны в список опрашиваемых диапазонов.

  Если включить параметр **Использовать Zeroconf для опроса IPv6-сетей**, точка распространения выполняет опрос IPv6-сети, используя сеть с нулевой конфигурацией (далее также *Zeroconf*). В этом случае указанные IP-диапазоны игнорируются, так как точка распространения опрашивает всю сеть. Параметр **Использовать Zeroconf для опроса IPv6-сетей** доступен, если точка распространения работает под управлением Linux. Чтобы использовать опрос Zeroconf IPv6, 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 результате выбранные устройства будут выполнять роль точек распространения.

Только устройства под управлением операционной системы Windows могут определять свое сетевое местоположение. Определение сетевого местоположения недоступно для устройств под управлением других операционных систем.

Удаление устройства из списка точек распространения

Чтобы удалить устройство из списка точек распространения:

1. В дереве консоли выберите узел **Сервер администрирования**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Точки распространения** выберите устройство, выполняющее функции точки распространения, и нажмите на кнопку **Удалить**.

В результате устройство будет удалено из списка точек распространения и перестанет выполнять функции точки распространения.

Невозможно удалить устройство из списка точек распространения, если оно было назначено Сервером администрирования автоматически.

Загрузка обновлений точками распространения

Kaspersky Security Center позволяет точкам распространения получать обновления от Сервера администрирования, серверов "Лаборатории Касперского", из локальной или сетевой папки.

Если вам не нужно указывать источник обновлений, рекомендуется использовать задачу *Загрузка обновлений в хранилища точек распространения* для группы администрирования. Дополнительную информацию см. в разделе Создание задачи загрузки обновлений в хранилища точек распространения.

Чтобы настроить получение обновлений для точки распространения:

1. В дереве консоли выберите узел **Сервер администрирования**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Точки распространения** выберите точку распространения, через которую обновления будут доставляться на клиентские устройства группы.
4. По кнопке **Свойства** откройте окно свойств выбранной точки распространения.
5. В окне свойств точки распространения выберите раздел **Источники обновлений**.
6. Выберите источник обновлений для точки распространения:
   - Чтобы точка распространения получала обновления с Сервера администрирования, выберите вариант **Получать с Сервера администрирования**:
     - **Загрузить файлы различий**

       Этот параметр включает функцию загрузки файлов различий.

       По умолчанию параметр включен.

- Чтобы точка распространения получала обновления с помощью задачи, выберите вариант **Использовать задачу принудительной загрузки обновлений**:

  - Нажмите на кнопку **Выбрать**, если такая задача уже есть на устройстве, и выберите задачу в появившемся списке.

  - Нажмите на кнопку **Новая задача**, чтобы создать задачу, если такой задачи еще нет на устройстве. Запустится мастер создания задачи. Следуйте далее указаниям мастера.

  Задача загрузки обновлений в хранилища точек распространения является локальной. Для каждого устройства, выполняющего роль точки распространения, задачу требуется создавать отдельно.

В результате точка распространения будет получать обновления из указанного источника.

Удаление обновлений программного обеспечения из хранилища

Чтобы удалить обновления программного обеспечения из хранилища Сервера администрирования:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Обновления программного обеспечения**.

2. В рабочей области папки **Обновления программного обеспечения** выберите обновление, которое нужно удалить.

3. В контекстном меню обновления выберите **Удалить файлы обновлений**.

Обновления программного обеспечения будут удалены из хранилища Сервера администрирования.

Установка патча для приложения "Лаборатории Касперского" в кластерной модели

Kaspersky Security Center поддерживает только ручную установку патчей для приложений "Лаборатории Касперского" в кластерной модели.

Чтобы установить патч для приложения "Лаборатории Касперского":

1. Загрузите на каждый узел кластера патч.

2. Запустите установку патча на активном узле.

3. Дождитесь успешной установки патча.

4. Последовательно запустите патч на всех подчиненных узлах кластера.

   При запуске патча из командной строки используйте ключ `-CLUSTER_SECONDARY_NODE`.

В результате этих действий патч будет установлен на каждом узле кластера.

5. Запустите вручную кластерные службы "Лаборатории Касперского".

Каждый узел кластера будет отображаться в Консоли администрирования как устройство с установленным Агентом администрирования.

Информацию об установленных патчах можно просмотреть в папке **Обновления программного обеспечения** или в отчете о версиях обновлений модулей приложений "Лаборатории Касперского".

Управление приложениями сторонних производителей на клиентских устройствах

Kaspersky Security Center позволяет управлять приложениями "Лаборатории Касперского" и других производителей, установленными на клиентских устройствах.

Администратор может выполнять следующие действия:

- создавать категории приложений на основании заданных критериев;
- управлять категориями приложений с помощью специально созданных правил;
- управлять запуском приложений на устройствах;
- выполнять инвентаризацию и вести реестр программного обеспечения, установленного на устройствах;
- закрывать уязвимости программного обеспечения, установленного на устройствах;
- устанавливать обновления Windows Update и других производителей программного обеспечения на устройствах;
- отслеживать использование лицензионных ключей для групп лицензионных приложений.

О приложениях сторонних производителей

Kaspersky Security Center может помочь вам обновить приложения сторонних производителей, установленные на клиентских устройствах, и закрыть уязвимости в приложениях сторонних производителей. Kaspersky Security Center 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, просмотрев список доступных обновлений в Консоли администрирования на основе консоли Microsoft Management Console (MMC) и в Kaspersky Security Center Web Console.

Процедура ниже предназначена для просмотра списка стороннего программного обеспечения, которое можно обновить с помощью Kaspersky Security Center. 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 в Kaspersky Security Center Web Console:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. На шаге мастера **Параметры новой задачи** укажите следующие параметры:
   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Security Center**.
   b. В поле **Тип задачи** выберите **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.

Чтобы просмотреть список приложений сторонних производителей, которые вы можете обновить с помощью Kaspersky Security Center в Консоли администрирования на основе консоли Microsoft Management Console (MMC), вам потребуется лицензия на Системное администрирование. Иначе задача **Установка требуемых обновлений и закрытие уязвимостей** будет недоступна.

1. В дереве консоли выберите папку **Управляемые устройства**.
2. В рабочей области выберите вкладку **Задачи**.
3. По кнопке **Создать задачу** запустите мастер создания задачи. Следуйте далее указаниям мастера.
4. На странице мастера **Выбор типа задачи** выберите **Установка требуемых обновлений и закрытие уязвимостей**.
5. На шаге мастера **Задайте правила установки обновлений** нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.
6. На шаге мастера **Выбор типа правила** выберите параметр **Правило для сторонних обновлений**.
7. На шаге мастера **Общие критерии** выберите параметр **Устанавливать все обновления, кроме отклоненных** и нажмите на кнопку **Далее**.

Отобразится список приложений сторонних производителей.

Установка обновлений приложений сторонних производителей

Kaspersky Security Center позволяет управлять обновлениями программного обеспечения, установленного на клиентских устройствах, и закрывать уязвимости в приложениях Microsoft и других производителей программного обеспечения с помощью установки необходимых обновлений.

Kaspersky Security Center выполняет поиск обновлений с помощью задачи поиска обновлений и загружает обновления в хранилище обновлений. После завершения поиска обновлений приложение предоставляет администратору информацию о доступных обновлениях и об уязвимостях в приложениях, которые можно закрыть с помощью этих обновлений.

Информация о доступных обновлениях Microsoft Windows передается из центра обновлений Windows. Сервер администрирования может использоваться в роли сервера Windows Update (WSUS). Для использования Сервера администрирования в роли сервера Windows Update необходимо настроить синхронизацию обновлений с центром обновлений Windows. После настройки синхронизации данных с центром обновлений Windows Сервер администрирования с заданной периодичностью централизованно предоставляет обновления службам Windows Update на устройствах.

Управлять обновлениями программного обеспечения можно также с помощью политики Агента администрирования. Для этого необходимо создать политику Агента администрирования и настроить параметры обновлений программного обеспечения в соответствующих окнах мастера создания политики.

Администратор может просматривать список доступных обновлений в папке **Обновления программного обеспечения**, входящей в состав папки **Управление приложениями**. Эта папка содержит список полученных Сервером администрирования обновлений приложений Microsoft и других производителей программного обеспечения, которые могут быть распространены на устройства. После просмотра информации о доступных обновлениях администратор может выполнить установку обновлений на устройства.

Обновление некоторых приложений Kaspersky Security Center выполняет путем удаления предыдущей версии приложения и установки новой версии.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Убедитесь, что параметр **Отображать Системное администрирование** включен в окне **Настройка интерфейса** для главного и подчиненного Серверов администрирования. Иначе задача поиска обновлений обрабатывает только обновления WSUS.

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.

Перед установкой обновлений на все устройства можно выполнить проверочную установку, чтобы убедиться, что установленные обновления не вызовут сбоев в работе приложений на устройствах.

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.

Предварительные требования

Сервер администрирования должен иметь подключение к интернету для установки обновлений приложений сторонних производителей, отличных от приложений Microsoft.

По умолчанию Сервер администрирования не требует подключения к интернету для установки обновлений приложений Microsoft на управляемые устройства. Например, управляемые устройства могут загружать обновления приложений Microsoft непосредственно с серверов обновлений Microsoft или с Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации. Если вы используете Сервер администрирования в качестве сервера WSUS, Сервер администрирования должен быть подключен к интернету.

Этапы

Обновление производителей состоит из следующих этапов:

1. **Поиск требуемых обновлений**

   Чтобы найти обновления приложений сторонних производителей, необходимые для управляемых устройств, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Kaspersky Security Center получает списки обнаруженных уязвимостей и требуемых обновлений для 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:

   - Консоль администрирования: Поиск уязвимостей в приложениях, Задание расписания для задачи поиска уязвимостей и требуемых обновлений.
   - Kaspersky Security Center Web Console: Создание задачи Поиск уязвимостей и требуемых обновлений, Параметры задачи поиска уязвимостей и требуемых обновлений.

2. **Анализ списка найденных обновлений**

Просмотрите список **Обновления программного обеспечения** 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 клиентских устройствах.

Инструкции:

- Консоль администрирования: Просмотр информации о доступных обновлениях.
- Kaspersky Security Center Web Console: Просмотр информации о доступных обновлениях приложений сторонних производителей.

3. **Настройка установки обновлений**

После того как Kaspersky Security Center получает список обновлений приложений сторонних производителей, вы можете установить их на клиентские устройства, используя задачу *Установка требуемых обновлений и закрытия 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 программного обеспечения**.

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для установки обновлений для приложений Microsoft, включая обновления, предоставляемые службой Центра обновления Windows, и обновления приложений других поставщиков. Обратите внимание, что эту задачу можно создать, только если у вас есть лицензия на Системное администрирование.

Задача *Установка обновлений Центра обновления Windows* не требует лицензии, но ее можно использовать только для установки обновлений Центра обновления Windows.

Для установки некоторых обновлений программного обеспечения вам нужно принять Лицензионное соглашение для установки программного обеспечения. Если вы отклоните Лицензионное соглашение, обновления программного обеспечения не будут установлены.

Вы можете запустить задачу установки обновления по расписанию. При указании расписания задачи убедитесь, что задача установки обновления запускается после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

Инструкции:

- Консоль администрирования: Закрытие уязвимостей в приложениях, Просмотр информации о доступных обновлениях.
- Kaspersky Security Center Web Console: 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, задача *Поиск уязвимостей и требуемых обновлений* настроена на запуск вручную.

Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете задать ее запуск с той же периодичностью или реже, что и запуск задачи *Поиск уязвимостей и требуемых обновлений*. 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 установки обновлений запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

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.

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.

По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус на *Одобрено* или *Отклонено* в списке **Обновления программного обеспечения** (**Операции → Управление патчами → Обновления программного обеспечения**).

Инструкции:

- Консоль администрирования: Одобрение и отклонение обновлений программного обеспечения.
- Kaspersky Security Center Web Console: Одобрение и отклонение обновлений приложений сторонних производителей.

6. **Настройка Сервера администрирования для работы в качестве службы Windows Server Update Services (WSUS) (если требуется)**

   По умолчанию обновления Центра обновления Windows загружаются на управляемые устройства с серверов Microsoft. Вы можете изменить этот параметр, чтобы использовать Сервер администрирования в роли WSUS-сервера. В этом случае Сервер администрирования синхронизирует данные обновления с Центром обновления Windows с заданной периодичностью и предоставляет обновления централизовано службам Центра обновления Windows на сетевых устройствах.

   Чтобы использовать Сервер администрирования в качестве сервера WSUS, создайте задачу Синхронизация обновлений Windows Update и установите флажок **Использовать Сервер администрирования в роли WSUS-сервера** в политике Агента администрирования.

   Инструкции:

   - Консоль администрирования: Синхронизация обновлений Windows Update с Сервером администрирования, Настройка обновлений Windows в политике Агента администрирования.
   - Kaspersky Security Center Web Console: Создание задачи Синхронизация обновлений Windows Update.

7. **Запуск задачи установки обновлений**

   Запустите задачу *Установка требуемых обновлений и закрытия 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*.

8. **Создание отчета о результатах установки обновлений приложений сторонних производителей (если требуется)**

   Чтобы просмотреть статистику установки обновления, сформируйте **Отчет о результатах установки обновлений стороннего ПО**.

Инструкции:

- Консоль администрирования: Создание и просмотр отчета.
- Kaspersky Security Center Web Console: Генерация и просмотр отчета.

Результаты

Если вы создали и настроили задачу *Установка требуемых обновлений и закрытия уязвимостей*, обновления будут автоматически установлены на управляемые устройства. При загрузке новых обновлений в хранилище Сервера администрирования Kaspersky Security Center проверяет, соответствуют ли они критериям, указанным в правилах обновлений. Все новые обновления, которые соответствуют критериям, будут установлены автоматически при следующем запуске задачи.

Если вы создали задачу *Установка обновлений Центра обновления Windows*, будут установлены только те обновления, которые указаны в свойствах задачи *Установка обновлений Центра обновления Windows*. Позже, если вы захотите установить новые обновления, загруженные в хранилище Сервера администрирования, вам будет необходимо добавить требуемые обновления в список обновлений существующей задачи или создать задачу *Установка обновлений Центра обновления Windows*.

Просмотр информации о доступных обновлениях для приложений сторонних производителей

Чтобы просмотреть список доступных обновлений для приложений сторонних производителей, установленных на клиентских устройствах,

В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Обновления программного обеспечения**.

В рабочей области папки вы можете просматривать список имеющихся обновлений для приложений, установленных на устройствах.

Чтобы просмотреть свойства обновления,

в рабочей области папки **Обновления программного обеспечения** в контекстном меню обновления выберите пункт **Свойства**.

В окне свойств обновления для просмотра доступна следующая информация:

- В разделе **Общие** вы можете просмотреть **Статус одобрения обновления**:
  - **Не определено** – обновление доступно в списке обновлений, но не одобрено для установки.
  - **Одобрено** – обновление доступно в списке обновлений и одобрено к установке.
  - **Отклонено** – обновление отклонено для установки.

- В разделе **Атрибуты** вы можете просмотреть значения поля **Устанавливаемый автоматически**:
  - Значение **Автоматически** отображается, если задача *Установка требуемых обновлений и закрытие уязвимостей* может устанавливать обновления для приложения. Задача автоматически устанавливает новые обновления с веб-адреса, предоставленного поставщиком приложений сторонних производителей.
  - Значение **Вручную** отображается, если Kaspersky Security Center не может установить обновления для приложения автоматически. Вы можете установить обновления вручную.

  Поле **Устанавливаемый автоматически** не отображается для обновлений приложений Windows.

- Список клиентских устройств, для которых применимо обновление.
- Список системных компонентов (предварительных требований), которые должны быть установлены перед обновлением (любым).
- Уязвимости в приложениях, которые закрывают это обновление.

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.

Для управления установкой обновлений приложений сторонних производителей использование статуса *Одобрено* целесообразно для небольшого количества обновлений. Чтобы установить несколько обновлений приложений сторонних производителей, 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 дереве консоли выберите узел **Дополнительно → Управление приложениями → Обновления программного обеспечения**.
2. В рабочей области папки **Обновления программного обеспечения** перейдите по ссылке **Обновить** вверху справа и дождитесь загрузки списка обновлений. Отобразится список обновлений.
3. Выберите обновления, которые требуется подтвердить или отклонить.

   Блок работы с выбранным объектом отображается в правой части рабочей области.
4. В раскрывающемся списке **Статус одобрения обновления** выберите **Одобрено**, чтобы подтвердить выбранные обновления, или **Отклонено**, чтобы отменить выбранные обновления.

   По умолчанию указано значение **Не определено**.

Обновления, для которых установлен статус **Одобрено**, помещаются в очередь на установку.

Обновления, для которых установлен статус **Отклонено**, деинсталлируются (если это возможно) с устройств, на которые они были ранее установлены. Также они не будут установлены на устройства позже.

Некоторые обновления для приложений "Лаборатории Касперского" невозможно деинсталлировать. Если вы установили для них статус **Отклонено**, Kaspersky Security Center не будет деинсталлировать эти обновления с устройств, на которые они были установлены ранее. Такие обновления никогда не будут установлены на устройства в будущем. Если обновления для приложений "Лаборатории Касперского" не могут быть удалены, это свойство отображается в окне свойств обновления. В панели **Разделы** выберите **Общие**, и свойство отобразится в разделе **Требования к установке** рабочей области. 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.

Синхронизация обновлений Windows Update с Сервером администрирования

Если в окне **Использовать Сервер администрирования в роли WSUS-сервера** мастера первоначальной настройки вы выбрали вариант **Параметры управления обновлениями**, задача синхронизации с Центром обновления Windows создается автоматически. Запустить задачу можно в папке **Задачи**. Функция обновления программного обеспечения Microsoft доступна только после успешного завершения задачи **Синхронизация обновлений Windows Update**.

Обновления программного обеспечения Microsoft могут превышать 10 ГБ. Убедитесь, что база данных Сервера администрирования способна вместить такие тома, иначе задача **Синхронизация обновлений Windows Update** не будет выполнена. База данных Microsoft SQL Express не поддерживается для задачи **Синхронизация обновлений Windows Update**.

Задача **Синхронизация обновлений Windows Update** загружает с серверов Microsoft только метаданные. Если в сети не используется WSUS-сервер, то каждое клиентское устройство самостоятельно загружает обновления Microsoft с внешних серверов.

Чтобы создать задачу синхронизации обновлений Windows Update с Сервером администрирования:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Обновления программного обеспечения**.

2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите значение **Настроить синхронизацию обновлений Windows Update**.

   В мастере создается задача **Синхронизация обновлений Windows Update**, отображаемая в папке **Задачи**.

   Запустится мастер создания задачи получения данных из центра обновлений Windows. Следуйте далее указаниям мастера.

Задачу синхронизации обновлений Windows Update также можно создать в папке **Задачи** по кнопке **Создать задачу**.

Microsoft периодически удаляет со своих серверов устаревшие обновления, так что число актуальных обновлений составляет от 200 000 до 300 000. Для уменьшения используемого дискового пространства и размера базы данных Kaspersky Security Center удаляет устаревшие обновления, которые отсутствуют на серверах обновлений Microsoft.

Во время выполнения задачи **Синхронизация обновлений Windows Update**, приложение получает список актуальных обновлений с сервера обновлений Microsoft. После чего Kaspersky Security Center определяет список устаревших обновлений. При следующем запуске задачи **Поиск уязвимостей и требуемых обновлений** Kaspersky Security Center отмечает устаревшие обновления и устанавливает время на удаление. При следующем запуске задачи **Синхронизация обновлений Windows Update** удаляются обновления, которые были отмечены на удаление 30 дней назад. Kaspersky Security Center также выполняет дополнительную проверку для удаления устаревших обновлений, которые были отмечены на удаление более 180 дней назад.

После завершения работы задачи **Синхронизация обновлений Windows Update** и удаления устаревших обновлений в базе данных могут оставаться хеш-коды файлов удаленных обновлений, а также соответствующие им файлы в папке %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles, в случае если они были загружены ранее. С помощью задачи **Обслуживание Сервера администрирования** можно удалить такие устаревшие записи из базы данных и соответствующие им файлы.

Шаг 1. Определение необходимости уменьшения трафика

Когда Kaspersky Security Center синхронизирует обновления с серверами Microsoft Windows Update Servers, информация обо всех файлах сохраняется в базе данных Сервера администрирования. Также на диск загружаются все файлы, необходимые для обновления, при взаимодействии с Агентом обновления Windows. В частности, Kaspersky Security Center сохраняет информацию о файлах экспресс-установки в базу данных и загружает их по мере необходимости. Загрузка файлов экспресс-установки приводит к сокращению свободного места на диске.

Чтобы уменьшить сокращение объема дискового пространства и снизить трафик, вы можете выключить параметр **Загружать файлы экспресс-установки**.

Если параметр выбран, в процессе выполнения задачи загружаются файлы экспресс-установки. По умолчанию вариант не выбран.

Шаг 2. Приложения

В этом разделе можно выбрать приложения, для которых будут загружаться обновления.

Если установлен флажок **Все приложения**, то обновления будут загружаться для всех имеющихся приложений, а также для тех приложений, которые могут быть выпущены в будущем.

По умолчанию флажок **Все приложения** установлен.

Шаг 3. Категории обновлений

В этом разделе можно выбрать категории обновлений, которые будут загружаться на Сервер администрирования.

Если установлен флажок **Все категории**, то обновления будут загружаться для всех имеющихся категорий обновлений, а также для тех категорий, которые могут появиться в будущем.

По умолчанию флажок **Все категории** установлен.

Шаг 4. Языки локализации обновлений

В этом окне можно выбрать языки локализации обновлений, которые будут загружаться на Сервер администрирования. Выберите один из следующих вариантов загрузки языков локализации обновлений:

- **Загружать все языки, включая новые**

  Если выбран этот вариант, на Сервер администрирования будут загружаться все доступные языки локализации обновлений. По умолчанию выбран этот вариант.

- **Загружать выбранные языки**

  Если выбран этот вариант, в списке можно выбрать языки локализации обновлений, которые должны загружаться на Сервер администрирования.

Шаг 5. Выбор учетной записи для запуска задачи

В окне **Выбор учетной записи для запуска задачи** можно указать, под какой учетной записью запускать задачу. Выберите один из следующих вариантов:

- **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.

Шаг 6. Настройка расписания запуска задачи

В окне **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

  Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

  - **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.

  - **Каждые N минут**

    Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

    По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

  - **Ежедневно (не поддерживается переход на летнее время)**

    Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

    Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

    По умолчанию задача запускается каждый день в текущее системное время.

  - **Еженедельно**

    Задача запускается каждую неделю в указанный день и в указанное время.

  - **По дням недели**

    Задача выполняется регулярно, в указанные дни недели, в указанное время.

    По умолчанию задача запускается каждую пятницу в 18:00:00.

  - **Ежемесячно**

    Задача выполняется регулярно, в указанный день месяца, в указанное время.

    В месяцах, у которых нет указанного дня, задача выполняется в последний день.

    По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

  По умолчанию выбран этот вариант.

- **Один раз**

  Задача выполняется один раз, в указанные дату и время (по умолчанию в день создания задачи).

- **Ежемесячно, в указанные дни выбранных недель**

  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 случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

Шаг 7. Определение названия задачи

В окне **Определение названия задачи** укажите название создаваемого правила. Название задачи не может превышать 100 символов и не может содержать специальные символы (`"*<>?\:|`). Значение по умолчанию – *Синхронизация обновлений Windows Update*.

Шаг 8. Завершение создания задачи

В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

Созданная задача синхронизации обновлений Windows Update отобразится в списке задач в папке **Задачи** дерева консоли.

Установка обновлений на устройства вручную

Если в окне **Параметры управления обновлениями** мастера первоначальной настройки вы выбрали вариант **Искать и устанавливать требующиеся обновления**, задача *Установка требуемых обновлений и закрытие уязвимостей* создается автоматически. Остановить или запустить задачу можно в папке **Управляемые устройства** на вкладке **Задачи**.

Если в мастере первоначальной настройки вы выбрали вариант **Искать требуемые обновления**, вы можете установить обновления программного обеспечения на клиентские устройства с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей*.

Вы можете выполнить одно из следующих действий:

- Создайте задачу для установки обновлений.
- Добавьте правило для установки обновления в существующую задачу установки обновлений.
- В параметрах существующей задачи установки обновлений настройте тестовую установку обновлений.

> Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Установка обновлений с помощью создания задачи установки обновлений

Вы можете выполнить одно из следующих действий:

- Создайте задачу для установки требуемых обновлений.
- Выберите обновление и создайте задачу для его установки и для установки аналогичных обновлений.

Чтобы установить требуемые обновления:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Обновления программного обеспечения**.
2. В рабочей области папки выберите обновление, которое вы хотите установить.

3. Выполните одно из следующих действий:

   - В контекстном меню выбранного обновления выберите пункт **Установить обновление → Новая задача**.

   - По ссылке **Установить обновление (создать задачу)** в блоке работы с выбранными файлами.

4. Откроется окно установки всех предыдущих версий приложения. Нажмите **Да**, если вы согласны на последовательную установку версий приложения, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить приложение, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

   Откроется мастер создания задачи установки обновлений и закрытия уязвимостей. Следуйте далее указаниям мастера.

5. В окне мастера **Выбор действия при необходимости перезагрузки операционной системы** выберите действие, которое необходимо выполнить, если операционная система на клиентских устройствах должна быть перезапущена после операции:

   - **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.

- **Принудительное закрытие приложения в заблокированных сессиях через (мин)**

  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.

6. На странице **Настройка расписания запуска задачи** мастера можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

   - **Запуск по расписанию:**

     Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

     - **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.

     - **Каждые N минут**

       Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

       По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

     - **Ежедневно (не поддерживается переход на летнее время)**

       Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

  По умолчанию выбран этот вариант.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию 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 случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

7. На странице **Определение названия задачи** мастера укажите название создаваемой задачи. Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

8. На странице **Завершение создания задачи** мастера нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

В результате работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**.

Вы можете включить автоматическую установку общесистемных компонентов (пререквизитов), перед установкой обновления в свойствах задачи *Установка требуемых обновлений и закрытие уязвимостей*. Когда параметр включен, все требуемые общесистемные компоненты устанавливаются перед обновлением. Список этих компонентов можно посмотреть в свойствах обновления.

В свойствах задачи *Установка требуемых обновлений и закрытие уязвимостей* вы можете разрешить установку обновлений, которые обновляют приложение до новой версии.

Если в параметрах задачи настроены правила установки обновлений сторонних производителей, Сервер администрирования загружает с сайта производителей требуемые обновления. Обновления сохраняются в хранилище Сервера администрирования и далее распространяются и устанавливаются на устройства, где они применимы.

Если в параметрах задачи настроены правила установки обновлений Microsoft и Сервер администрирования используется в качестве WSUS-сервера, Сервер администрирования загружает необходимые обновления в хранилище и далее распространяет на управляемые устройства. Если в сети не используется WSUS-сервер, то каждое клиентское устройство самостоятельно загружает обновления Microsoft с внешних серверов.

Чтобы установить требуемое обновление и аналогичные обновления:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Обновления программного обеспечения**.

2. В рабочей области выберите обновление, которое вы хотите установить.

3. Нажмите на кнопку **Запустить мастер установки обновления**.

   Запустится мастер установки обновления.

   > Функционал мастера установки обновления доступен при наличии лицензии на Системное администрирование.

   Следуйте далее указаниям мастера.

4. На странице **Поиск существующих задач установки обновления** укажите следующие параметры:

   - **Искать задачи, устанавливающие выбранное обновление**

     Если этот параметр включен, мастер установки обновления ищет существующую задачу, чтобы установить выбранное обновление.

     Если этот параметр выключен или если не было найдено подходящей задачи, мастер установки обновления предлагает создать правило или задачу для установки обновления.

По умолчанию параметр включен.

- **Одобрить установку 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.

5. Если вы выбрали поиск существующей задачи для установки обновлений и было найдено несколько подходящих задач, вы можете просмотреть свойства этих задач или запустить их вручную. Никаких дальнейших действий не требуется.

   В противном случае нажмите на кнопку **Новая задача установки обновления**.

6. Выберите тип правила установки, чтобы добавить его в новую задачу и нажмите на кнопку **Готово**.

7. Откроется окно установки всех предыдущих версий приложения. Нажмите **Да**, если вы согласны на последовательную установку версий приложения, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить приложение, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

   Откроется мастер создания задачи установки обновлений и закрытия уязвимостей. Следуйте далее указаниям мастера.

8. В окне мастера **Выбор действия при необходимости перезагрузки операционной системы** выберите действие, которое необходимо выполнить, если операционная система на клиентских устройствах должна быть перезапущена после операции:

   - **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.

- **Принудительное закрытие приложения в заблокированных сессиях через (мин)**

  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. На странице мастера **Выбор устройств, которым будет назначена задача** выберите один из следующих вариантов:

   - **Выбрать устройства, обнаруженные в сети Сервером администрирования**

     В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

     Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

   - **Задать адреса устройств вручную или импортировать из списка**

     Вы можете задавать 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.

   - **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.

10. На странице **Настройка расписания запуска задачи** мастера можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

  Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

  - **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.

  - **Каждые N минут**

    Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

    По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

  - **Ежедневно (не поддерживается переход на летнее время)**

    Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

    Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

    По умолчанию задача запускается каждый день в текущее системное время.

  - **Еженедельно**

    Задача запускается каждую неделю в указанный день и в указанное время.

  - **По дням недели**

    Задача выполняется регулярно, в указанные дни недели, в указанное время.

По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную** (выбрано по умолчанию)

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

  По умолчанию выбран этот вариант.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию 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 случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

11. На странице **Определение названия задачи** мастера укажите название создаваемой задачи. Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

12. На странице **Завершение создания задачи** мастера нажмите на кнопку **Готово**, чтобы завершить работу мастера.

    Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

После завершения работы мастера создается задача **Установка требуемых обновлений и закрытие**

уязвимостей, которая отображается в папке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

После установки новой версии приложения может быть нарушена работа других приложений, установленных на устройствах и зависящих от работы обновляемого приложения.

Установка обновления с помощью добавления правила в существующую задачу

Чтобы установить обновление с помощью добавления правила в существующую задачу:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Обновления программного обеспечения**.
2. В рабочей области выберите обновление, которое вы хотите установить.
3. Нажмите на кнопку **Запустить мастер установки обновления**.

   Запустится мастер установки обновления.

   Функционал мастера установки обновления доступен при наличии лицензии на Системное администрирование.

   Следуйте далее указаниям мастера.
4. На странице **Поиск существующих задач установки обновления** укажите следующие параметры:

   - **Искать задачи, устанавливающие выбранное обновление**

     Если этот параметр включен, мастер установки обновления ищет существующую задачу, чтобы установить выбранное обновление.

     Если этот параметр выключен или если не было найдено подходящей задачи, мастер установки обновления предлагает создать правило или задачу для установки обновления.

     По умолчанию параметр включен.

   - **Одобрить установку 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.
5. Если вы выбрали поиск существующей задачи для установки обновлений и было найдено несколько подходящих задач, вы можете просмотреть свойства этих задач или запустить их вручную. Никаких дальнейших действий не требуется.

   В противном случае нажмите на кнопку **Добавить правило установки обновления**.

6. Выберите задачу, для которой вы хотите добавить правило и нажмите на кнопку **Добавить правило**.

   Также вы можете просмотреть свойства существующих задач, запустить их вручную или создать задачу.

7. Выберите тип правила, которое будет добавлено в выбранную задачу, и нажмите на кнопку **Готово**.

8. Откроется окно установки всех предыдущих версий приложения. Нажмите **Да**, если вы согласны на последовательную установку версий приложения, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить приложение, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

Новое правило для установки обновления добавлено в существующую задачу **Установка требуемых обновлений и закрытие уязвимостей**.

Настройка проверочной установки обновлений

Чтобы настроить проверочную установку обновлений:

1. В дереве консоли в папке **Управляемые устройства** на вкладке **Задачи** выберите задачу **Установка требуемых обновлений и закрытие уязвимостей**.

2. В контекстном меню задачи выберите пункт **Свойства**.

   Откроется окно свойств задачи **Установка требуемых обновлений и закрытие уязвимостей**.

3. В окне свойств задачи в разделе **Проверочная установка** выберите один из доступных вариантов проверочной установки:

   - **Не проверять**. Выберите этот вариант, если вы не хотите выполнять проверочную установку обновлений.

   - **Выполнить проверку на указанных устройствах**. Выберите этот вариант, если вы хотите проверить установку обновлений на определенных устройствах. Нажмите на кнопку **Добавить** и выберите устройства, на которых нужно выполнить проверочную установку обновлений.

   - **Выполнить проверку на устройствах в указанной группе**. Выберите этот вариант, если вы хотите проверить установку обновлений на группе устройств. В поле **Задайте тестовую группу** укажите группу устройств, на которых нужно выполнить проверочную установку.

   - **Выполнить проверку на указанном проценте устройств**. Выберите этот вариант, если вы хотите выполнить проверку обновлений на части устройств. В поле **Процент тестовых устройств из общего числа устройств** укажите процент устройств, на которых нужно выполнить проверочную установку обновлений.

4. После выбора любого параметра, кроме **Не проверять**, в поле **Среднее время для принятия решения о продолжении установки (ч)** укажите количество часов, которое должно пройти от тестовой установки обновлений, до начала установки обновлений на все устройства.

Настройка обновлений Windows в политике Агента администрирования

Чтобы настроить обновления Windows в политике Агента администрирования:

1. В дереве консоли выберите **Управляемые устройства**.
2. В рабочей области выберите вкладку **Политики**.
3. Выберите политику Агента администрирования.
4. В контекстном меню политики выберите пункт **Свойства**.

   Откроется окно свойств политики Агента администрирования.
5. В панели **Разделы** выберите **Обновления и уязвимости в приложениях**.
6. Выберите параметр **Использовать Сервер администрирования в роли WSUS-сервера**, чтобы загружать обновления Windows на Сервер администрирования и затем распространять их на клиентские устройства средствами Агента администрирования.

   Если этот параметр не выбран, обновления Windows загружаются на Сервер администрирования. В этом случае клиентские устройства получают обновления Windows напрямую с серверов Microsoft.
7. Выберите набор обновлений, которые могут устанавливать пользователи на своих устройствах вручную, используя Центр обновления Windows.

   Для устройств с операционными системами Windows 10, если в Центре обновления Windows уже найдены обновления для устройств, то новый параметр, который вы выбрали под **Разрешить пользователям управлять установкой обновлений Центра обновления Windows**, будет применен только после установки найденных обновлений.

   Выберите параметр из раскрывающегося списка:

   - **Устанавливать все применимые обновления Центра обновления Windows**

     Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам.

     Выберите этот вариант, если вы не хотите влиять на установку обновлений.

     Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

   - **Устанавливать только одобренные обновления Центра обновления Windows**

     Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам и которые одобрены администратором.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом разрешить установку этих одобренных обновлений на клиентских устройствах.

Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

- **Запретить устанавливать обновления Центра обновления Windows**

  Пользователи не могут устанавливать обновления Центра обновления Windows на своих устройства вручную. Все применимые обновления устанавливаются в соответствии с настройкой, заданной администратором.

  Выберите этот вариант, если вы хотите централизованно управлять установкой обновлений.

  Например, вы можете настроить расписание обновления так, чтобы не загружать сеть. Вы можете запланировать обновления вне рабочего времени, чтобы они не мешали производительности пользователей.

8. Выберите режим поиска обновлений Windows Update:

   - **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.

9. Выберите параметр **Проверять исполняемые файлы на наличие уязвимостей при запуске**, если требуется выполнять проверку исполняемых файлов на наличие уязвимостей при запуске.

10. Убедитесь, что редактирование заблокировано для всех параметров, которые вы изменили. В противном случае изменения не применяются.

11. Нажмите на кнопку **Применить**.

Закрытие уязвимостей в приложениях сторонних производителей

В этом разделе описаны возможности Kaspersky Security Center связанные с закрытием уязвимостей в приложениях, установленных на управляемых устройствах.

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей

В этом разделе представлен сценарий обнаружения и закрытия уязвимостей на управляемых устройствах под управлением Windows. Вы можете обнаружить и закрыть уязвимости в операционной системе и в стороннем программном обеспечении, включая программное обеспечение Microsoft.

Предварительные требования

- Kaspersky Security Center развернут в вашей организации.
- В сети вашей организации есть управляемые устройства под управлением Windows.
- Подключение Сервера администрирования к интернету необходимо для выполнения следующих задач:
  - Составление списка рекомендуемых исправлений уязвимостей в приложениях Microsoft. Список формируется и регулярно обновляется специалистами "Лаборатории Касперского".
  - Закрытие уязвимостей в приложениях сторонних производителей, отличных от приложений Microsoft.

Этапы

Обнаружение и закрытие уязвимостей состоит из следующих этапов:

1. **Поиск уязвимостей в программном обеспечении, установленном на управляемых устройствах**

   Чтобы найти уязвимости в приложениях, установленных на управляемых устройствах, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Kaspersky Security Center получает 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. Если вы не запускали мастер первоначальной настройки, запустите его сейчас или создайте задачу вручную.

Инструкции:

- Консоль администрирования: Поиск уязвимостей в приложениях, Задание расписания для задачи поиска уязвимостей и требуемых обновлений.
- Kaspersky Security Center Web Console: Создание задачи Поиск уязвимостей и требуемых обновлений, Параметры задачи поиска 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:

- Консоль администрирования: Просмотр информации об уязвимостях в приложениях, Просмотр статистики уязвимостей на управляемых устройствах.
- Kaspersky Security Center Web Console: 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. Обратите внимание, что эту задачу можно создать, только если у вас есть лицензия на Системное администрирование. Чтобы устранить уязвимости в приложениях, задача *Установка требуемых обновлений и закрытие уязвимостей* использует рекомендованные обновления приложений.

Задача *Закрытие уязвимостей* не требует лицензии для Системного администрирования. Чтобы использовать эту задачу, требуется вручную указать пользовательские исправления для закрытия уязвимостей в приложениях сторонних производителей, которые указаны в параметрах задачи. Задача *Закрытие уязвимостей* использует рекомендованные исправления приложений Microsoft и пользовательские исправления для приложений сторонних производителей.

Вы можете запустить мастер закрытия уязвимостей, который автоматически создаст одну из этих задач, или вы можете создать одну из этих задач вручную.

Инструкции:

- Консоль администрирования: Пользовательские исправления для уязвимостей в приложениях сторонних производителей, Закрытие уязвимостей в приложениях.
- Kaspersky Security Center Web Console: Пользовательские исправления для уязвимостей в приложениях сторонних производителей, 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 или реже, что и запуск задачи *Поиск уязвимостей и требуемых обновлений*. При задании расписания задачи *Закрытие уязвимостей*, вам нужно выбрать исправления приложений Microsoft или указать пользовательские исправления для приложений сторонних производителей каждый раз перед запуском задачи.

При задании расписания задач убедитесь, что задача закрытия уязвимостей запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

5. **Игнорирование уязвимостей в приложениях (если требуется)**

   Вы можете игнорировать уязвимости в приложениях, которые должны быть закрыты на всех управляемых устройствах или только на выбранных управляемых устройствах.

   Инструкции:

   - Консоль администрирования: Игнорирование уязвимостей в приложениях.
   - Kaspersky Security Center Web Console: Игнорирование уязвимостей в приложениях.

6. **Запуск задачи закрытия уязвимости**

   Запустите задачу *Установка требуемых обновлений и закрытия уязвимостей* или *Закрытие уязвимостей*. Когда задача будет завершена, убедитесь, что в списке задач она имеет статус *Завершена успешно*.

7. **Создание отчета о результатах закрытия уязвимостей в приложениях (если требуется)**

   Чтобы просмотреть статистику о закрытых уязвимостях, сформируйте отчет об уязвимостях. 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.

   Инструкции:

   - Консоль администрирования: Создание и просмотр отчета.
   - Kaspersky Security Center Web Console: Генерация и просмотр отчета.

8. **Проверка настройки обнаружения и закрытия уязвимостей в приложениях сторонних производителей**

   Убедитесь, что вы выполнили следующее:

   - обнаружили и просмотрели список уязвимостей в приложениях на управляемых устройствах;
   - игнорировали уязвимости в приложениях, если хотели;
   - настроили задачу закрытия уязвимости;
   - запланировали запуск задач для поиска и закрытия уязвимостей в приложениях так, чтобы они запускались последовательно;
   - проверили, что задача закрытия уязвимостей была запущена.

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 в правилах, будут загружены в хранилище Сервера администрирования и будут установлены для закрытия уязвимостей в приложениях.

Если вы создали задачу *Закрытие уязвимостей*, закрываются только уязвимости в приложениях Microsoft.

Об обнаружении и закрытии уязвимостей в приложениях

Kaspersky Security Center 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 выполняет поиск известных уязвимостей в приложениях на основе признаков из баз данных об известных уязвимостях. Эта база формируются 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 для поиска уязвимостей в приложениях используется задача *Поиск уязвимостей и требуемых обновлений*.

В некоторых случаях обнаруженные уязвимости в операционной системе Microsoft Windows можно закрыть одним из следующих способов:

- Установить обновления для операционной системы.
- Обновить операционную систему до новой версии (например, с Windows 10 до Windows 11).

В этом сценарии Kaspersky Security Center отображает две записи для одной и той же уязвимости.

Закрытие уязвимостей в приложениях

Для закрытия уязвимостей в приложениях, Kaspersky Security Center использует обновления программного обеспечения выпущенные поставщиками программного обеспечения. Метаданные обновлений программного обеспечения загружаются в хранилище Сервера администрирования в результате выполнения следующих задач:

- *Загрузка обновлений в хранилище Сервера администрирования*. Эта задача предназначена для загрузки метаданных обновлений для приложений "Лаборатории Касперского" и приложений сторонних производителей. Эта задача автоматически создается в мастере первоначальной настройки Kaspersky Security Center. Задача загрузки обновлений в хранилище Сервера администрирования может быть создана вручную.

- *Синхронизация обновлений Windows Update*. Эта задача предназначена для загрузки метаданных обновлений программного обеспечения Microsoft.

Обновления программного обеспечения для закрытия уязвимостей могут быть представлены в виде полных дистрибутивов или патчей. Обновления программного обеспечения, которые закрывают уязвимости в приложениях, называются *исправлениями*. *Рекомендуемые исправления* это исправления, которые рекомендуются к установке специалистами "Лаборатории Касперского". *Пользовательские исправления* это исправления, которые вручную указываются для установки пользователями. Чтобы установить пользовательское исправление, необходимо создать инсталляционный пакет, содержащий это исправление.

Если лицензия Kaspersky Security Center предусматривает возможности Системного администрирования, для закрытия уязвимостей используйте задачу *Установка требуемых обновлений и закрытие уязвимостей*. Эта задача автоматически закрывает несколько уязвимостей, устанавливая рекомендуемые исправления. Для этой задачи вы можете вручную настроить определенные правила для закрытия нескольких уязвимостей.

Если лицензия Kaspersky Security Center не предусматривает возможности Системного администрирования, для закрытия уязвимостей используйте задачу *Закрытие уязвимостей*. С помощью этой задачи можно закрыть уязвимости, установив рекомендуемые исправления для приложений Microsoft и пользовательских исправлений для приложений сторонних производителей.

Из соображений безопасности любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных приложений с помощью технологий "Лаборатории Касперского". Эти технологии используются для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение.

Эксперты "Лаборатории Касперского" не проводят ручной анализ обновлений приложений сторонних производителей, которые можно установить с помощью Системного администрирования. Также эксперты "Лаборатории Касперского" не занимаются поиском уязвимостей (известных или неизвестных) или недокументированных возможностей в таких обновлениях и не проводят другие виды анализа упомянутых выше обновлений.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Для закрытия некоторых уязвимостей программного обеспечения вам нужно принять Лицензионное соглашение для установки программного обеспечения, если это требуется. Если вы отклоняете Лицензионное соглашение, уязвимость в программном обеспечении не закроется.

Просмотр информации об уязвимостях в приложениях

Чтобы просмотреть список уязвимостей, обнаруженных на клиентских устройствах,

В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Уязвимости в приложениях**.

Отобразится страница со списком уязвимостей в приложениях, обнаруженных на управляемых устройствах.

Чтобы получить информацию о выбранной уязвимости,

В контекстном меню уязвимости выберите пункт **Свойства**.

Откроется окно свойств уязвимости, в котором отображается следующая информация:

- приложение, в котором обнаружена уязвимость;
- список устройств, на которых обнаружена уязвимость;
- информация о закрытии уязвимости.

Чтобы просмотреть отчет обо всех обнаруженных уязвимостях,

В папке **Уязвимости в приложениях** перейдите по ссылке **Просмотреть отчет об уязвимостях в приложениях**.

Будет создан отчет об уязвимостях в приложениях, установленных на устройствах. Отчет можно просмотреть в узле с именем нужного вам Сервера администрирования на вкладке **Отчеты**.

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 дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Уязвимости в приложениях**.

   Отобразится страница со списком уязвимостей в приложениях, обнаруженных на управляемых устройствах.

2. Выберите уязвимость для которой вы хотите просмотреть статистику.

   В блоке для работы с выбранным объектом отображается диаграмма состояний уязвимости. Нажав на статус, откроется список устройств, на которых уязвимость имеет выбранный статус.

Поиск уязвимостей в приложениях

Если вы выполнили настройку приложения с помощью мастера первоначальной настройки, задача *Поиск уязвимостей* создается автоматически. Просмотреть задачу можно в папке **Управляемые устройства** на вкладке **Задачи**.

Чтобы создать задачу поиска уязвимостей в приложениях, установленных на клиентских устройствах:

1. В дереве консоли выберите **Дополнительно** → **Управление приложениями**, а затем выберите подпапку **Уязвимости в приложениях**.

2. В рабочей области выберите **Дополнительные действия** → **Настроить поиск уязвимостей**.

   Если задача для поиска уязвимостей уже существует, она отображается на вкладке **Задачи** в папке **Управляемые устройства**, с существующими выбранными задачами. В противном случае запускается мастер создания задачи Поиск уязвимостей и требуемых обновлений. Следуйте далее указаниям мастера.

3. В окне **Выбор типа задачи** выберите **Поиск уязвимостей и требуемых обновлений**.

4. В окне мастера **Параметры**, укажите следующие параметры задачи:

   - **Поиск уязвимостей и обновлений, перечисленных Microsoft**

     При поиске уязвимостей и обновлений Kaspersky Security Center использует данные о применимых обновлениях Microsoft из источника обновлений Microsoft, доступного в текущий момент.

     Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft и обновлений сторонних приложений.

     По умолчанию параметр включен.

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 (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 не запрашивает информацию об обновлениях.

- **Поиск уязвимостей и сторонних обновлений, перечисленных "Лабораторией Касперского"**

  Если этот параметр включен, Kaspersky Security Center выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите пути для дополнительного поиска приложений в файловой системе**. Полный список поддерживаемых приложений сторонних производителей контролируется "Лабораторией Касперского".

  Если этот параметр выключен, Kaspersky Security Center не выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних приложений.

  По умолчанию параметр включен.

- **Укажите пути для дополнительного поиска приложений в файловой системе**

  Папки, в которых Kaspersky Security Center выполняет поиск сторонних приложений, требующих закрытия уязвимостей и установки обновлений. Вы можете использовать системные переменные.

  Укажите папки, в которые были установлены приложения. По умолчанию список содержит системные папки, в которые устанавливается большинство приложений.

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать файлы трассировки, даже если запись файлов трассировки выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

  При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

  По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

  По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

5. На странице **Настройка расписания запуска задачи** мастера можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

   - **Запуск по расписанию:**

     Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

     - **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.

     - **Каждые N минут**

       Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживается переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

  По умолчанию выбран этот вариант.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию указано время 18:00 и не выбраны дни месяца.

  > Обратите внимание, что вы выбираете порядковый номер дня недели в месяце, а не конкретную дату в месяце или номер недели (первая, вторая неделя месяца). Например, если вы выберите ячейку **Вт** в строке **Первая**, в этом случае задача будет запускаться каждый первый вторник каждого нового месяца.

  Вы можете выбрать несколько дней недели.

- **При загрузке обновлений в хранилище**

  Эта задача запускается после загрузки обновлений в хранилище. Например, вам может понадобиться это расписание для задачи поиска уязвимостей и требуемых обновлений.

- **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 случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

6. На странице **Определение названия задачи** мастера укажите название создаваемой задачи. Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

7. На странице **Завершение создания задачи** мастера нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

В результате работы мастера создается задача **Поиск уязвимостей и требуемых обновлений**, которая отображается в списке задач, в папке **Управляемые устройства**, на вкладке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

Когда задача *Поиск уязвимостей и требуемых обновлений* завершена, Сервер администрирования отображает список уязвимостей, обнаруженных в приложениях, установленных на устройстве; также Сервер отображает все обновления программного обеспечения, необходимые для исправления обнаруженных уязвимостей.

Если отображается ошибка 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", решить эту проблему можно с помощью реестра Windows.

Сервер администрирования не отображает список необходимых обновлений программного обеспечения при последовательном запуске двух задач: задачи *Синхронизация обновлений Windows Update*, для которой отключен параметр **Загружать файлы экспресс-установки**, и затем задачи *Поиск уязвимостей и требуемых обновлений*. Чтобы просмотреть список необходимых обновлений программного обеспечения, необходимо снова запустить задачу *Поиск уязвимостей и требуемых обновлений*.

Агент администрирования получает информацию о любых доступных обновлениях Windows и других приложений Microsoft от Центра обновления Windows или от Сервера администрирования, если Сервер администрирования выполняет роль WSUS-сервера. Информация передается при запуске приложений (если это предусмотрено политикой) и при каждом запуске задачи *Поиск уязвимостей и требуемых обновлений* на клиентских устройствах.

Закрытие уязвимостей в приложениях

Если в окне **Параметры управления обновлениями** мастера первоначальной настройки вы выбрали вариант **Искать и устанавливать требующиеся обновления**, задача *Установка требуемых обновлений и закрытие уязвимостей* создается автоматически. Задача отображается в папке **Управляемые устройства** на вкладке **Задачи**.

В противном случае вы можете выполнить одно из следующих действий:

- Создайте задачу для закрытия уязвимостей с помощью установки доступных обновлений.
- Добавьте правило для закрытия уязвимостей в существующую задачу закрытия уязвимостей.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Закрытие уязвимостей с помощью задачи закрытия уязвимостей

Вы можете выполнить одно из следующих действий:

- Создайте задачу закрытия нескольких уязвимостей, соответствующих определенным правилам.
- Выберите уязвимость и создайте задачу для ее закрытия и для закрытия аналогичных уязвимостей.

Чтобы закрыть уязвимости, которые соответствуют определенным правилам:

1. В дереве консоли выберите Сервер администрирования, на устройствах которого вы хотите закрыть уязвимости.
2. В меню **Вид** главного окна приложения выберите пункт **Настройка интерфейса**.
3. В открывшемся окне установите флажок **Отображать Системное администрирование** и нажмите на кнопку **OK**.
4. В окне с сообщением приложения нажмите на кнопку **OK**.
5. Перезапустите Консоль администрирования, чтобы изменения вступили в силу.
6. В дереве консоли выберите папку **Управляемые устройства**.
7. В рабочей области выберите вкладку **Задачи**.
8. По кнопке **Создать задачу** запустите мастер создания задачи. Следуйте далее указаниям мастера.

9. В окне **Выбор типа задачи** мастера создания задачи выберите **Установка требуемых обновлений и закрытие уязвимостей**.

   Если задача не отображается, проверьте, есть ли у вашей учетной записи права **Чтение**, **Изменение** и **Выполнение** в функциональной области **Управление системой**: **Системное администрирование**. Вы не можете создавать и настраивать задачу *Установка требуемых обновлений и закрытие уязвимостей* без этих прав доступа.

10. В окне мастера **Параметры**, укажите следующие параметры задачи:

    - **Задайте правила установки обновлений**

      Эти правила применяются при установке обновлений на клиентские устройства. Если правила не указаны, задача не выполняется. Дополнительную информацию о работе с правилами см. в разделе Правила установки обновлений.

    - **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.

    - **Загружать обновления на устройство, не устанавливая их**

      Если флажок установлен, приложение загружает обновления на устройство, но не устанавливает их автоматически. Затем вы можете вручную установить загруженные обновления.

      Обновления Microsoft загружаются в служебную папку Windows. Обновления сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) загружаются в папку, указанную в поле **Загрузить обновления для**.

      Если этот параметр выключен, обновления автоматически устанавливаются на устройство.

По умолчанию параметр выключен.

- **Загрузить обновления для**

  Эта папка используется для загрузки обновлений сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft).

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать файлы трассировки, даже если запись файлов трассировки выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

  При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

  По умолчанию параметр выключен.

  - **Максимальный размер файлов расширенной диагностики, МБ**

    По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

11. В окне мастера **Выбор действия при необходимости перезагрузки операционной системы** выберите действие, которое необходимо выполнить, если операционная система на клиентских устройствах должна быть перезапущена после операции:

    - **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.

- **Принудительное закрытие приложения в заблокированных сессиях через (мин)**

  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.

12. На странице **Настройка расписания запуска задачи** мастера можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

    - **Запуск по расписанию:**

      Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

      - **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.

- **Каждые N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживается переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

  По умолчанию выбран этот вариант.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

По умолчанию 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 случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

13. На странице **Определение названия задачи** мастера укажите название создаваемой задачи. Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

14. На странице **Завершение создания задачи** мастера нажмите на кнопку **Готово**, чтобы завершить работу мастера.

    Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

В результате работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

Если результаты задачи содержат ошибку 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", решить эту проблему можно с помощью реестра Windows.

Чтобы закрыть требуемую уязвимость и аналогичные ей:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Уязвимости в приложениях**.

2. Выберите уязвимость, которую вы хотите закрыть.

3. Нажмите на кнопку **Запустить мастер закрытия уязвимости**.

   Откроется мастер закрытия уязвимости.

Функционал мастера закрытия уязвимости доступен при наличии лицензии на Системное администрирование.

Следуйте далее указаниям мастера.

4. В разделе **Поиск существующих задач закрытия уязвимости** укажите следующие параметры:

   - **Показывать только задачи, закрывающие выбранную уязвимость**

     Если этот параметр включен, мастер закрытия уязвимости выполняет поиск существующих задач для закрытия выбранной уязвимости.

     Если этот параметр выключен или не было найдено применимых задач, мастер закрытия уязвимости предлагает создать правило или задачу для закрытия уязвимости.

     По умолчанию параметр включен.

   - **Одобрить обновления, закрывающие выбранную уязвимость**

     Обновления, которые закрывают уязвимость, будут одобрены к установке. Включите этот параметр, если некоторые применяемые правила установки обновлений разрешают установку только одобренных обновлений.

     По умолчанию параметр выключен.

5. Если для закрытия уязвимости вы выбрали поиск существующих задач и было найдено несколько задач, вы можете просмотреть свойства этих задач или запустить их вручную. Никаких дальнейших действий не требуется.

   В противном случае нажмите на кнопку **Новая задача закрытия уязвимости**.

6. Выберите тип правила, закрывающего уязвимость, чтобы добавить его в существующую задачу и нажмите на кнопку **Готово**.

7. Откроется окно установки всех предыдущих версий приложения. Нажмите **Да**, если вы согласны на последовательную установку версий приложения, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить приложение, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

   Откроется мастер создания задачи установки обновлений и закрытия уязвимостей. Следуйте далее указаниям мастера.

8. В окне мастера **Выбор действия при необходимости перезагрузки операционной системы** выберите действие, которое необходимо выполнить, если операционная система на клиентских устройствах должна быть перезапущена после операции:

   - **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.

- **Принудительное закрытие приложения в заблокированных сессиях через (мин)**

  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. На странице мастера **Выбор устройств, которым будет назначена задача** выберите один из следующих вариантов:

   - **Выбрать устройства, обнаруженные в сети Сервером администрирования**

     В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

     Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

- **Задать адреса устройств вручную или импортировать из списка**

  Вы можете задавать 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.

- **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.

10. На странице **Настройка расписания запуска задачи** мастера можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

    - **Запуск по расписанию:**

      Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

      - **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.

- **Каждые N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживается переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

  По умолчанию выбран этот вариант.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию 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 случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

11. На странице **Определение названия задачи** мастера укажите название создаваемой задачи. Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

12. На странице **Завершение создания задачи** мастера нажмите на кнопку **Готово**, чтобы завершить работу мастера.

    Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

В результате работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

Закрытие уязвимости с помощью добавления правила в существующую задачу закрытия уязвимостей

Чтобы закрыть уязвимость с помощью добавления правила в существующую задачу закрытия уязвимостей:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Уязвимости в приложениях**.

2. Выберите уязвимость, которую вы хотите закрыть.

3. Нажмите на кнопку **Запустить мастер закрытия уязвимости**.

   Откроется мастер закрытия уязвимости.

   > Функционал мастера закрытия уязвимости доступен при наличии лицензии на Системное администрирование.

   Следуйте далее указаниям мастера.

4. В разделе **Поиск существующих задач закрытия уязвимости** укажите следующие параметры:

   - **Показывать только задачи, закрывающие выбранную уязвимость**

     Если этот параметр включен, мастер закрытия уязвимости выполняет поиск существующих задач для закрытия выбранной уязвимости.

     Если этот параметр выключен или не было найдено применимых задач, мастер закрытия уязвимости предлагает создать правило или задачу для закрытия уязвимости.

     По умолчанию параметр включен.

   - **Одобрить обновления, закрывающие выбранную уязвимость**

     Обновления, которые закрывают уязвимость, будут одобрены к установке. Включите этот параметр, если некоторые применяемые правила установки обновлений разрешают установку только одобренных обновлений.

     По умолчанию параметр выключен.

5. Если для закрытия уязвимости вы выбрали поиск существующих задач и было найдено несколько задач, вы можете просмотреть свойства этих задач или запустить их вручную. Никаких дальнейших действий не требуется.

   В противном случае нажмите на кнопку **Добавить правило закрытия уязвимости в существующую задачу**.

6. Выберите задачу, для которой вы хотите добавить правило и нажмите на кнопку **Добавить правило**.

   Также вы можете просмотреть свойства существующих задач, запустить их вручную или создать задачу.

7. Выберите тип правила, чтобы добавить его в выбранную задачу, и нажмите на кнопку **Готово**.

8. Откроется окно установки всех предыдущих версий приложения. Нажмите **Да**, если вы согласны на последовательную установку версий приложения, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить приложение, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

Новое правило для закрытия уязвимости добавлено в существующую задачу **Установка требуемых обновлений и закрытие уязвимостей**.

Закрытие уязвимостей в изолированной сети

В этом разделе описаны действия, которые вы можете предпринять для закрытия уязвимостей в приложениях сторонних производителей на управляемых устройствах, подключенных к Серверам администрирования и не имеющих доступа в интернет.

Сценарий: закрытие уязвимостей в приложениях сторонних производителей в изолированной сети

Вы можете устанавливать обновления и закрывать уязвимости приложений сторонних производителей, установленных на управляемых устройствах в изолированной сети. К таким сетям относятся Серверы администрирования и подключенные к ним управляемые устройства, не имеющие доступа в интернет. Для закрытия уязвимостей в такой сети необходим Сервер администрирования, подключенный к интернету. Также вы можете загружать патчи (требуемые обновления) с помощью Сервера администрирования с доступом в интернет и передавать исправления на изолированные Серверы администрирования.

Вы можете загружать обновления приложений сторонних производителей, выпущенные производителями программного обеспечения, но не можете загружать обновления для программного обеспечения Microsoft на изолированных Серверах администрирования с помощью Kaspersky Security Center.

Чтобы узнать, как работает процесс закрытия уязвимостей в изолированной сети, ознакомьтесь с описанием и схемой этого процесса.

Предварительные требования

Перед началом сделайте следующее:

1. Выделите одно устройство для подключения к интернету и загрузки исправлений. Это устройство будет считаться Сервером администрирования с доступом в интернет.
2. Установите Kaspersky Security Center версии не ниже 14 на следующих устройствах:
   - Выделенное устройство, которое будет выступать в роли Сервера администрирования с доступом в интернет.
   - Изолированные устройства, которые будут выступать в роли изолированных от интернета Серверов администрирования (далее – изолированные Серверы администрирования).
3. Убедитесь, что на каждом Сервере администрирования достаточно места на диске для загрузки и хранения обновлений и исправлений.

Этапы

Установка обновлений и закрытие уязвимостей приложений сторонних производителей на управляемых устройствах, относящихся к изолированным Серверам администрирования, состоит из следующих этапов:

1. **Настройка Сервера администрирования с доступом в интернет**

   Подготовьте Сервер администрирования с доступом в интернет для обработки запросов на необходимые обновления стороннего программного обеспечения и для загрузки.

2. **Настройка изолированных Серверов администрирования**

   Подготовьте изолированные Серверы администрирования, чтобы они могли регулярно формировать списки необходимых обновлений и обрабатывать патчи, загружаемые Сервером администрирования с доступом в интернет. После настройки изолированные Серверы администрирования больше не пытаются загружать патчи из интернета. Вместо этого они получают обновления через патчи.

3. **Передача патчей и установка обновлений на изолированные Серверы администрирования**

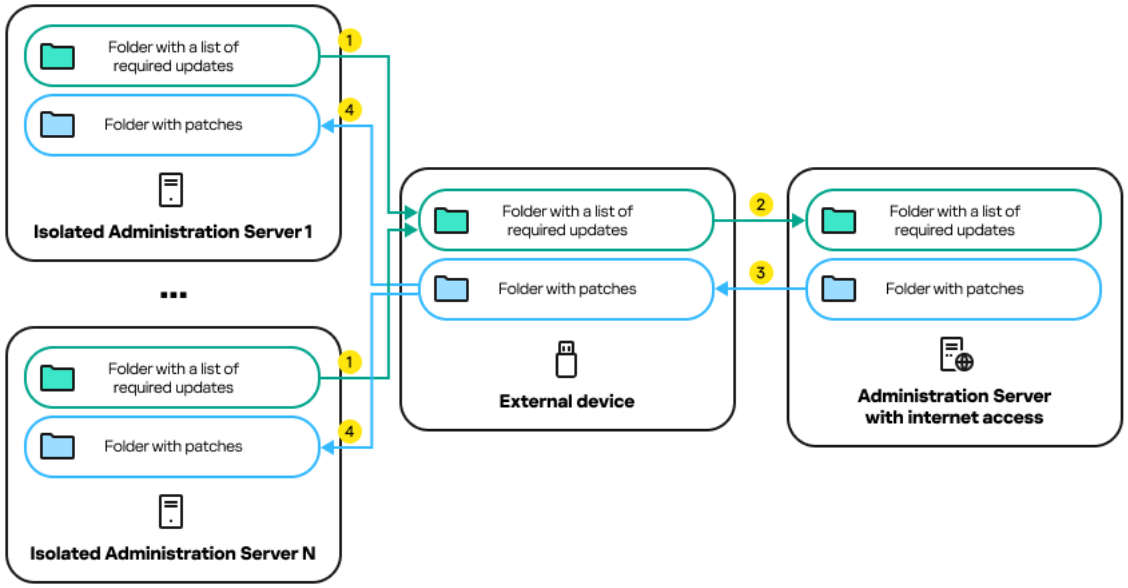
   После завершения настройки Серверов администрирования вы можете передавать необходимые списки обновлений и патчей между Сервером администрирования с доступом в интернет и изолированными Серверами администрирования. Далее обновления из исправлений будут установлены на управляемые устройства с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей*.

Результаты

Таким образом обновления приложений сторонних производителей передаются на изолированные Серверы администрирования и устанавливаются на подключенные управляемые устройства с помощью Kaspersky Security Center. Достаточно один раз настроить Серверы администрирования, чтобы получать обновления с нужной вам частотой, например, один или несколько раз в день.

О закрытии уязвимостей в приложениях сторонних производителей в изолированной сети

Процесс закрытия уязвимостей в приложениях сторонних производителей в изолированной сети показан на рисунке и описан ниже. Вы можете периодически повторять этот процесс.



Процесс передачи патчей и списка необходимых обновлений между Сервером администрирования с доступом в интернет и изолированными Серверами администрирования

Каждый Сервер администрирования, изолированный от сети интернет (далее – изолированный Сервер администрирования), формирует список обновлений, которые необходимо установить на управляемые устройства, подключенные к данному Серверу администрирования. Список необходимых обновлений хранится в специальной папке и представляет собой набор бинарных файлов. Каждый файл имеет имя, которое содержит идентификатор патча с требуемым обновлением. В результате каждый файл в списке указывает на определенный патч.

С помощью внешнего устройства вы переносите список необходимых обновлений с изолированного Сервера администрирования на выделенный Сервер администрирования с доступом в интернет. После этого выделенный Сервер администрирования загружает патчи из интернета и помещает их в отдельную папку.

Когда все патчи загружены и размещены в специальной для них папке, вы перемещаете патчи на каждый изолированный Сервер администрирования, с которого вы взяли список необходимых обновлений. Вы сохраняете патчи в специально созданную для них папку на изолированном Сервере администрирования. В результате задача *Установка требуемых обновлений и закрытие уязвимостей* запускает патчи и устанавливает обновления на управляемые устройства изолированных Серверов администрирования.

Настройка Сервера администрирования с доступом в интернет для закрытия уязвимостей в изолированной сети

Чтобы подготовиться к закрытию уязвимостей и передаче патчей в изолированной сети, сначала настройте Сервер администрирования с доступом в интернет, а затем настройте изолированные Серверы администрирования.

Чтобы настроить Сервер администрирования с доступом в интернет:

1. Создайте две папки на диске, где установлен Сервер администрирования:

   - папку для списка необходимых обновлений;
   - папку для патчей.

   Названия папок могут быть любыми.

2. Предоставьте группе KLAdmins право Изменение на созданные папки, используя стандартные средства администрирования операционной системы.

3. С помощью утилиты klscflag укажите пути к папкам в свойствах Сервера администрирования.

   Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

4. Введите следующие команды в командной строке Windows:

   - Чтобы указать путь к папке для исправлений:
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<path to the folder>"`
   - Чтобы задать путь к папке для списка необходимых обновлений:
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<path to the folder>"`

   Пример: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "C:\<папка для патчей>"`

5. При необходимости с помощью утилиты klscflag укажите, как часто Сервер администрирования должен проверять наличие новых запросов на исправления:
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <значение в секундах>`

   По умолчанию указано значение 120 секунд.

   Пример: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 150`

6. Создайте задачу *Поиск уязвимостей и требуемых обновлений*, чтобы получить информацию о патчах для приложений сторонних производителей, установленных на управляемых устройствах, и настройте расписание выполнения задачи.

7. Создайте задачу *Закрытие уязвимостей*, чтобы указать патчи для приложений сторонних производителей, используемых для закрытия уязвимостей, и настройте расписание задачи.

   Запустите задачи вручную, если вы хотите, чтобы они выполнялись раньше, чем указано в расписании задачи. Порядок запуска задач важен. Задачу *Закрытие уязвимостей* необходимо запустить после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

8. Перезапустите службу Сервера администрирования.

Теперь Сервер администрирования с доступом в интернет готов к загрузке и передаче обновлений на изолированные Серверы администрирования. Прежде чем приступить к закрытию уязвимостей, настройте изолированные Серверы администрирования.

Настройка изолированных Серверов администрирования для закрытия уязвимостей в изолированной сети

После того, как настройка Сервера администрирования с доступом в интернет закончена, подготовьте каждый изолированный Сервер администрирования в вашей сети, чтобы вы могли закрывать уязвимости и устанавливать обновления на управляемых устройствах, подключенных к изолированным Серверам администрирования.

Чтобы настроить изолированные Серверы администрирования, выполните следующие действия на каждом из них:

1. Активируйте лицензионный ключ для Системного администрирования.

2. Создайте две папки на диске, где установлен Сервер администрирования:

   - папку, в которой появится список необходимых обновлений;
   - папку для патчей.

   Названия папок могут быть любыми.

3. Предоставьте группе KLAdmins право *Изменение* на созданные папки, используя стандартные средства администрирования операционной системы.

4. С помощью утилиты klscflag укажите пути к папкам в свойствах Сервера администрирования.

   Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

5. Введите следующие команды в командной строке Windows:

   - Чтобы указать путь к папке для исправлений:
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<путь к папке>"`
   - Чтобы задать путь к папке для списка необходимых обновлений:
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<path to the folder>"`

   Пример: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "C:\<папка для патчей>"`

6. При необходимости с помощью утилиты klscflag укажите, как часто изолированный Сервер администрирования должен проверять наличие новых патчей:

```
klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <value in seconds>
```

По умолчанию указано значение 120 секунд.

Пример: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 150`

7. При необходимости с используйте утилиту klscflag для вычисления хешей SHA256 патчей:
   ```
   klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1
   ```
   Введя эту команду, вы можете убедиться, что патчи не были изменены при их переносе на изолированный Сервер администрирования и что вы получили корректные патчи, содержащие необходимые обновления.

   По умолчанию Kaspersky Security Center не вычисляет хеши SHA256 патчей. Если включить этот параметр, после получения патчей изолированным Сервером администрирования Kaspersky Security Center вычисляет их хеши и сравнивает полученные значения с хешами, хранящимися в базе данных Сервера администрирования. Если вычисленный хеш не совпадает с хешем в базе данных, возникает ошибка и вам необходимо заменить неверные патчи.

8. Создайте задачу *Поиск уязвимостей и требуемых обновлений*, чтобы получить информацию о патчах для приложений сторонних производителей, установленных на управляемых устройствах, и настройте расписание выполнения задачи.

9. Создайте задачу *Закрытие уязвимостей*, чтобы указать патчи для приложений сторонних производителей, используемых для закрытия уязвимостей, и настройте расписание задачи.

   Запустите задачи вручную, если вы хотите, чтобы они выполнялись раньше, чем указано в расписании задачи. Порядок запуска задач важен. Задачу *Закрытие уязвимостей* необходимо запустить после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

10. Перезапустите службу Сервера администрирования.

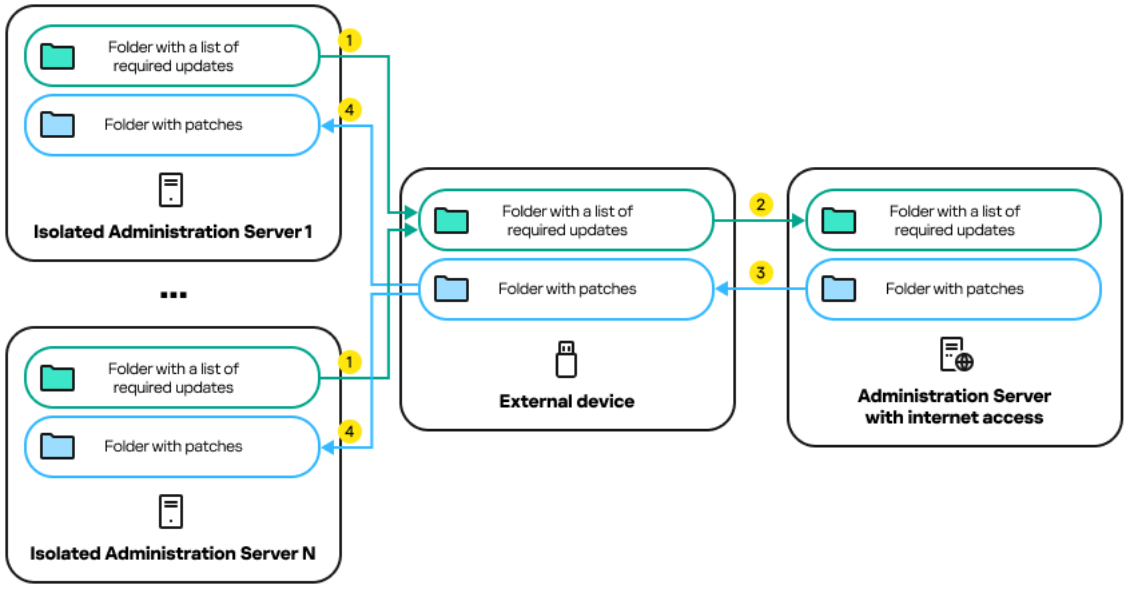
После настройки всех Серверов администрирования вы можете переместить исправления и списки необходимых обновлений и закрыть уязвимости приложений сторонних производителей на управляемых устройствах в изолированной сети.

Передача исправлений и установка обновлений в изолированной сети

После того, как настройка Серверов администрирования закончена, вы можете переносить патчи с необходимыми обновлениями с Сервера администрирования, имеющего доступ интернет, на изолированные Серверы администрирования. Вы можете передавать и устанавливать обновления с нужной вам частотой, например, один или несколько раз в день.

Съемный диск, например, внешний диск, необходим, для переноса патчей и списка необходимых обновлений между Серверами администрирования. Убедитесь, что внешний диск имеет достаточно места для загрузки и хранения патчей.

Процесс передачи патчей и списка необходимых обновлений показан на рисунке и описан ниже:



Процесс передачи патчей и списка необходимых обновлений между Сервером администрирования с доступом в интернет и изолированными Серверами администрирования

Чтобы установить обновления и закрыть уязвимости на управляемых устройствах, подключенных к изолированным Серверам администрирования:

1. Запустите задачу *Установка требуемых обновлений и закрытие уязвимостей*, если она еще не запущена.

2. Подключите внешний диск к любому изолированному Серверу администрирования.

3. Создайте на внешнем диске две папки: одну для списка необходимых обновлений и одну для патчей. Названия папок могут быть любыми.

   Если вы создали эти папки ранее, очистите их.

4. Скопируйте список необходимых обновлений с каждого изолированного Сервера администрирования и вставьте этот список в папку для списка необходимых обновлений на внешнем диске.

   В результате вы объединяете все списки, полученные со всех изолированных Серверов администрирования, в одну папку. В этой папке должны находиться бинарные файлы с идентификаторами патчей, необходимых для всех изолированных Серверов администрирования.

5. Подключите внешний диск к Серверу администрирования с доступом в интернет.

6. Скопируйте список необходимых обновлений с внешнего диска и вставьте этот список в папку для списка необходимых обновлений на Сервере администрирования с доступом в интернет.

   Все необходимые патчи автоматически загружаются из интернета в папку патчей на Сервере администрирования. Это может занять несколько часов.

7. Убедитесь, что все необходимые патчей загружены. Для этого можно выполнить одно из следующих действий:

   - Проверьте папку на наличие патчей на Сервере администрирования с доступом в интернет. Все исправления, которые были указаны в списке необходимых обновлений, должны быть загружены в нужную папку. Это удобнее, если требуется небольшое количество исправлений.

   - Подготовьте специальный скрипт, например, shell-скрипт. Если вы получите большое количество исправлений, то будет сложно самостоятельно проверить, что все исправления загружены. В таких случаях лучше автоматизировать проверку.

8. Скопируйте патчи с Сервера администрирования с доступом в интернет и вставьте их в соответствующую папку на внешнем диске.

9. Перенесите исправления на каждый изолированный Сервер администрирования. Поместите патчи в специальную папку для них.

В результате каждый изолированный Сервер администрирования формирует актуальный список обновлений, необходимых для управляемых устройств, подключенных к текущему Серверу администрирования. После получения списка необходимых обновлений Сервер администрирования загружает из интернета патчи. При появлении этих патчей на изолированных Серверах администрирования задача *Установка требуемых обновлений и закрытие уязвимостей* обрабатывает патчи. Таким образом, на управляемые устройства устанавливаются обновления и закрываются уязвимости в приложениях сторонних производителей.

При выполнении задачи *Установка требуемых обновлений и закрытие уязвимостей* не перезагружайте устройство Сервера администрирования и не запускайте задачу *Резервное копирование данных Сервера администрирования* (это также вызовет перезагрузку). В результате задача *Установка требуемых обновлений и закрытие уязвимостей* прерывается, а обновления не устанавливаются. В этом случае вам необходимо перезапустить эту задачу вручную или дождаться запуска задачи по настроенному расписанию.

Выключение возможности передачи исправлений и установки обновлений в изолированной сети

Вы можете выключить передачу исправлений на изолированные Сервера администрирования, например, если вы решили вывести один или несколько Серверов администрирования из изолированной сети. Таким образом вы сможете уменьшить количество исправлений и время на их загрузку.

Чтобы отключить возможность передачи патчей на изолированные Серверы администрирования:

1. Если вы хотите вывести из изоляции все Серверы администрирования, в свойствах Сервера администрирования с доступом в интернет удалите пути к папкам для патчей и список необходимых обновлений. Если вы хотите, чтобы некоторые Серверы администрирования находились в изолированной сети, пропустите этот шаг.

   Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Введите следующие команды в командной строке:

   - Чтобы удалить путь к папке с патчами:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```

- Чтобы удалить путь к папке со списком необходимых обновлений:
  ```
  klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
  ```

2. Перезапустите службу Сервера администрирования, если вы удалили пути к папкам на этом Сервере администрирования.

3. В свойствах каждого Сервера администрирования, который вы хотите вывести из изоляции, удалите пути к папкам для патчей и список необходимых обновлений.

   Введите следующие команды в командной строке Windows с правами администратора:

   - Чтобы удалить путь к папке с патчами:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
     ```

   - Чтобы удалить путь к папке со списком необходимых обновлений:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
     ```

4. Перезапустите службу каждого Сервера администрирования, на котором вы удалили пути к папкам.

Если вы перенастроили Сервер администрирования с доступом в интернет, вы больше не будете получать патчи через Kaspersky Security Center. Если вы перенастроили только некоторые изолированные Серверы администрирования, например, вынеся некоторые из них из изолированной сети, вы получите патчи только для остальных изолированных Серверов администрирования.

Если вы хотите в будущем приступить к закрытию уязвимостей на отключенных изолированных Серверах администрирования, вам необходимо настроить эти Серверы администрирования и Сервер администрирования с доступом в интернет еще раз.

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 дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Уязвимости в приложениях**.

   В рабочей области папки отображается список уязвимостей в приложениях на устройствах, которые обнаружил Агент администрирования, установленный на них.

2. Выберите уязвимость, которую вы хотите пропустить.

3. В контекстном меню уязвимости выберите пункт **Свойства**.

   Откроется окно свойств уязвимости.

4. В разделе **Общие** выберите параметр **Игнорировать уязвимость**.

5. Нажмите на кнопку **ОК**.

   Окно свойств уязвимости в приложениях закроется.

Уязвимость в приложениях пропускается на всех управляемых устройствах.

Чтобы пропустить уязвимость в приложениях на выбранных управляемых устройствах:

1. Откройте окно свойств выбранного управляемого устройства и выберите раздел **Уязвимости в приложениях**.

2. Выберите уязвимость в приложениях.

3. Пропустите выбранную уязвимость.

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.

Пользовательские исправления для уязвимостей в приложениях сторонних производителей

Чтобы использовать задачу *Закрытие уязвимостей*, необходимо вручную указать обновления программного обеспечения, чтобы закрыть уязвимости в приложениях сторонних производителей, перечисленные в параметрах задачи. Задача *Закрытие уязвимостей* использует рекомендованные исправления приложений Microsoft и пользовательские исправления для других приложений сторонних производителей. *Пользовательские исправления* это обновления программного обеспечения для закрытия уязвимостей, которые администратор вручную указывает для установки.

Чтобы выбрать пользовательские исправления для уязвимостей в приложениях сторонних производителей:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Уязвимости в приложениях**.

   В рабочей области папки отображается список уязвимостей в приложениях на устройствах, которые обнаружил Агент администрирования, установленный на них.

2. Выберите уязвимость для которой вы хотите указать пользовательское исправление.

3. В контекстном меню уязвимости выберите пункт **Свойства**.

   Откроется окно свойств уязвимости.

4. В разделе **Пользовательские и другие исправления** нажмите на кнопку **Добавить**.

   Отобразится список доступных инсталляционных пакетов. Список отобразившихся инсталляционных пакетов соответствует списку в папке **Удаленная установка** → **Инсталляционные пакеты**. Если вы не создали инсталляционный пакет, содержащий пользовательское исправление для закрытия выбранной уязвимости, вы можете создать пакет сейчас, запустив мастер создания инсталляционного пакета.

5. Выберите инсталляционный пакет (или пакеты), содержащий пользовательское исправление (или пользовательские исправления) для уязвимости приложениях сторонних производителей.

6. Нажмите на кнопку **OK**.

Указаны инсталляционные пакеты, содержащие пользовательские исправления для уязвимости в приложениях. После запуска задачи *Закрытие уязвимостей* будет установлен инсталляционный пакет и закрыта уязвимость в приложениях.

Правила установки обновлений

Для закрытия уязвимостей в приложениях, необходимо указать правила установки обновлений. Эти правила определяют обновления для установки и уязвимости к закрытию.

Точные параметры зависят от того, создаете ли вы правило для обновлений приложений Microsoft, приложений сторонних производителей (приложений, производимых поставщиками программного обеспечения, кроме "Лаборатории Касперского" и Microsoft) или всех приложений. При создании правила для приложений Microsoft или приложений сторонних производителей вы можете выбрать приложения и версии приложений, для которых вы хотите установить обновления. При создании правила для всех приложений вы можете выбрать обновления, которые необходимо установить, и уязвимости, которые необходимо закрыть с помощью установки обновлений.

Чтобы создать правило для обновления приложений:

1. В окне **Параметры** мастера создания задачи нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Следуйте далее указаниям мастера.

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 создаваемого 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 создастся и отобразится в поле **Задайте правила установки обновлений** мастера создания задачи.

Чтобы создать правило обновления приложений Microsoft:

1. В окне **Параметры** мастера создания задачи нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Следуйте далее указаниям мастера.

2. На странице **Тип правила** выберите **Правило для обновлений Windows Update**.

3. На странице **Общие критерии** укажите следующие параметры:

   - **Набор обновлений для установки**

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.

     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.

     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

     Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

     По умолчанию параметр выключен.

   - **Закрывать уязвимости с уровнем критичности по MSRC, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный Microsoft Security Response Center (MSRC), равен или превышает значение, выбранное в списке (**Низкий**, **Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

     Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

     По умолчанию параметр выключен.

4. В окне **Приложения** выберите приложения и версии приложений, для которых вы хотите установить обновления. По умолчанию выбраны все приложения.

5. В окне **Категории обновлений** выберите категории обновлений для установки. Эти категории такие же, как и в каталоге Центра обновления Microsoft. По умолчанию выбраны все категории.

6. В окне **Имя** укажите название создаваемого 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 создастся и отобразится в поле **Задайте правила установки обновлений** мастера создания задачи.

Чтобы создать правило для обновления приложений сторонних производителей:

1. В окне **Параметры** мастера создания задачи нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Следуйте далее указаниям мастера.

2. На странице **Тип правила** выберите **Правило для сторонних обновлений**.

3. На странице **Общие критерии** укажите следующие параметры:

   - **Набор обновлений для установки**

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.

     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.

     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

     Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

     По умолчанию параметр выключен.

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 создаваемого 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 создастся и отобразится в поле **Задайте правила установки обновлений** мастера создания задачи.

Группы приложений

В этом разделе описана работа с группами приложений, установленных на устройствах.

Создание категорий приложений

Kaspersky Security Center позволяет создавать категории приложений, установленных на устройствах.

Категории приложений можно создавать следующими способами:

- Администратор указывает папку, исполняемые файлы из которой попадают в выбранную категорию.
- Администратор указывает устройство, исполняемые файлы с которого попадают в выбранную категорию.
- Администратор задает критерии, по которым приложения попадают в выбранную категорию.

Когда категория приложений создана, администратор может задать правила для этой категории приложений. Правила определяют поведение приложений, входящих в указанную категорию. Например, можно запретить или разрешить запуск приложений, входящих в категорию.

Управление запуском приложений на устройствах

Kaspersky Security Center позволяет управлять запуском приложений на устройствах в режиме "Список разрешенных". Подробное описание приведено в справке Kaspersky Endpoint Security для Windows. В режиме "Список разрешенных" на выбранных устройствах разрешен запуск только тех приложений, которые входят в указанные категории. Администратор может просматривать результаты статического анализа правил запуска приложений на устройствах по каждому пользователю.

Инвентаризация программного обеспечения, установленного на устройствах

Kaspersky Security Center позволяет выполнять инвентаризацию программного обеспечения на устройствах под управлением Windows и Linux. Агент администрирования получает информацию обо всех приложениях, установленных на устройствах. Информация, полученная в результате инвентаризации, отображается в рабочей области папки **Реестр приложений**. Администратор может просматривать подробную информацию о каждом приложении, в том числе версию и производителя.

Количество исполняемых файлов, получаемых от одного устройства, не может превышать 150 000. При достижении этого ограничения Kaspersky Security Center не получит новые файлы.

Управление группами лицензионных приложений

Kaspersky Security Center позволяет создавать группы лицензионных приложений. В группу лицензионных приложений входят приложения, отвечающие критериям, заданным администратором. Администратор может указывать следующие критерии для групп лицензионных приложений:

- Название приложения.
- Версия приложения.
- Производитель.
- Тег приложения.

Приложения, соответствующие одному или нескольким критериям, автоматически попадают в группу. Для создания группы лицензионных приложений должен быть задан хотя бы один критерий включения приложений в эту группу.

Каждая группа лицензионных приложений имеет свой лицензионный ключ. Лицензионный ключ группы лицензионных приложений определяет допустимое количество установок для приложений, входящих в группу. Если количество установок превысило заданное в лицензионном ключе ограничение, на Сервере администрирования регистрируется информационное событие. Администратор может указать дату окончания действия лицензионного ключа. При наступлении этой даты на Сервере администрирования регистрируется информационное событие.

Просмотр информации об исполняемых файлах

Kaspersky Security Center получает всю информацию об исполняемых файлах, которые запускались на устройствах с момента установки на них операционной системы. Полученная информация об исполняемых файлах отображается в главном окне приложения в рабочей области папки **Исполняемые файлы**.

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.Также компонент доступен для Kaspersky Embedded Systems Security для Windows 3.0 и выше.

Предварительные требования

- Kaspersky Security Center развернут в вашей организации.
- Политика Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux создана и активна.
- Политика Kaspersky Embedded Systems Security для Windows или Kaspersky Embedded Systems 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.

   Инструкции:

   - Консоль администрирования: Инвентаризация исполняемых файлов.
   - Kaspersky Security Center Web Console: Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах.

2. **Создание категорий для исполняемых файлов, используемых в вашей организации**

   Проанализируйте списки приложений и 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.

   Инструкции:

   - Консоль администрирования: Создание пополняемой вручную категории приложений, Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств, Создание категории приложений, в которую входят исполняемые файлы из указанных папок.
   - Kaspersky Security Center Web Console: Создание пополняемой вручную категории приложений, Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств, Создание категории приложений, в которую входят исполняемые файлы из указанных папок.

3. **Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security**

   Настройте компонент Контроль приложений в политике Kaspersky Endpoint Security с использованием категорий, которые вы создали на предыдущем этапе.

Инструкции:

- Консоль администрирования: Настройка управления запуском приложений на клиентских устройствах.
- Kaspersky Security Center Web Console: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows.

4. **Настройка компонента Контроль приложений в политике Kaspersky Embedded Systems Security**

   Настройте компонент Контроль приложений в политике Kaspersky Embedded Systems Security для Windows, используя созданные вами категории. Подробную информацию о компоненте Контроль приложений см. в справке Kaspersky Embedded Systems Security для Windows или в справке Kaspersky Embedded Systems Security для Linux.

   При использовании большого количества правил может возникнуть ошибка при загрузке политики. Вы можете увеличить максимальный размер JSON-запроса в байтах, используя следующую команду:

   ```
   klscflag -fset -pv ".core/.independent" -s KLLIM -n
   LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v <max_request_size> -t d
   ```

   Где `<max_request_size>` это максимальный размер запроса в байтах (например, `200000000`).

5. **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 или Kaspersky Embedded Systems Security не будет блокировать исполняемые файлы, запуск которых запрещен правилами Контроля приложений, а вместо этого будет отправлять уведомления об их запуске на Сервер администрирования.

   При тестировании правил Контроля приложений рекомендуется выполнить следующие действия:

   - Определите период тестирования. Период тестирования может варьироваться от нескольких дней до двух месяцев.
   - Изучите события, возникающие в результате тестирования работы компонента Контроль приложений.

   Инструкции для Kaspersky Security Center Web Console: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows. Следуйте этой инструкции и включите параметр **Тестовый режим** в процессе настройки.

6. **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 пополняемую вручную.

   Инструкции:

   - Консоль администрирования: Добавление исполняемых файлов, связанных с событием, в категорию приложений.
   - Kaspersky Security Center Web Console: Добавление исполняемых файлов, связанных с событием, в категорию приложений.

7. **Применение правил Контроля приложений в рабочем режиме**

   После проверки правил Контроля приложений и завершения настройки категорий вы можете применить правила Контроль приложений в рабочем режиме.

   Инструкции для Kaspersky Security Center Web Console: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows. Следуйте этой инструкции и выключите параметр **Тестовый режим** в процессе настройки.

8. **Проверка конфигурации Контроля приложений**

   Убедитесь, что вы выполнили следующее:

   - Создали категории для исполняемых файлов.
   - Настроили Контроль приложений с использованием категорий.
   - Применили правила Контроля приложений в рабочем режиме.

Результаты

После завершения сценария, запуск исполняемых файлов на управляемых устройствах контролируется. Пользователи могут запускать только те исполняемые файлы, которые разрешены в вашей организации, и не могут запускать исполняемые файлы, запрещенные в вашей организации.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux
- Kaspersky Security для виртуальных сред Легкий агент
- Справка Kaspersky Embedded Systems Security для Windows
- Справка Kaspersky Embedded Systems Security для Linux

Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах

Вы можете получить список исполняемых файлов, хранящихся на клиентских устройствах, одним из следующих способов:

- Включив уведомление о запуске приложений в политике Kaspersky Endpoint Security.
- Создав задачу инвентаризации.

Включение уведомлений о запуске приложений в политике Kaspersky Endpoint Security

Чтобы включить уведомления о запуске приложения:

1. Откройте параметры политики Kaspersky Endpoint Security и перейдите на вкладку **Общие параметры** → **Отчеты и хранилища**.

2. В группе параметров **Передача данных на Сервер администрирования** установите флажок **О запущенных приложениях** и сохраните изменения.

   Когда пользователь пытается запустить исполняемые файлы, информация об этих файлах добавляется в список исполняемых файлов на клиентском устройстве. Kaspersky Endpoint Security отправляет эту информацию Агенту администрирования, а затем Агент администрирования отправляет ее на Сервер администрирования.

Создание задачи инвентаризации

Функция инвентаризации исполняемых файлов доступна для следующих приложений:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux версии 11.2 и выше
- Kaspersky Security для виртуальных сред 4.0 Легкий агент и выше

Вы можете снизить нагрузку на базу данных при получении информации об установленных приложениях. Чтобы сохранить дисковое пространство, запустите задачу инвентаризации на нескольких эталонных устройствах, на которых установлен стандартный набор приложений. Предпочтительное количество устройств равно 1–3.

> Настоятельно не рекомендуется выполнять задачу инвентаризации при использовании следующих баз данных: MySQL, PostgreSQL, SQL Server Express Edition, MariaDB (все версии).

Чтобы создать задачу инвентаризации исполняемых файлов на клиентских устройствах:

1. В дереве консоли выберите папку **Задачи**.

2. В рабочей области папки **Задачи** нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи.

3. В окне мастера **Выбор типа задачи** выберите тип задачи **Kaspersky Endpoint Security**, затем подтип задачи **Инвентаризация** и нажмите на кнопку **Далее**.

4. Следуйте дальнейшим шагам мастера.

   После того как мастер создания задачи завершит свою работу, задача **Инвентаризация** создана и настроена. Вы можете изменить параметры созданной задачи. В результате созданная задача отобразится в списке задач. Вы можете изменить параметры созданной задачи.

Подробное описание задачи инвентаризации см. в следующих справках:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux
- Kaspersky Security для виртуальных сред Легкий агент

После выполнения задачи **Инвентаризация** формируется список исполняемых файлов, хранящихся на управляемых устройствах, и вы можете просмотреть этот список.

Во время инвентаризации могут быть обнаружены исполняемые файлы в следующих форматах (в зависимости от выбранного вами параметра в свойствах задачи инвентаризации): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR и HTML.

Просмотр списка приложений и исполняемых файлов, хранящихся на управляемых устройствах

Чтобы просмотреть список исполняемых файлов, хранящихся на клиентских устройствах,

В дереве консоли перейдите в раздел **Дополнительно → Управление приложениями → Исполняемые файлы**.

При необходимости исполняемый файл можно отправить с управляемого устройства на устройство с установленной Консолью администрирования.

Чтобы отправить исполняемый файл:

1. В дереве консоли перейдите в раздел **Дополнительно → Управление приложениями → Исполняемые файлы**.
2. Перейдите по ссылке с исполняемым файлом, который требуется отправить на устройство с установленной Консолью администрирования.
3. В открывшемся окне перейдите в раздел **Устройства** и установите флажок рядом с управляемым устройством, с которого вы хотите отправить исполняемый файл.

   Перед отправкой исполняемого файла убедитесь, что управляемое устройство имеет прямое подключение к Серверу администрирования, установив флажок **Не разрывать соединение с Сервером администрирования**.

4. Нажмите кнопку **Отправить**, выберите папку назначения и нажмите кнопку **OK**.

   Выбранный исполняемый файл будет скачан для дальнейшей отправки на устройство с установленной Консолью администрирования.

Создание категорий приложений для политики Kaspersky Endpoint Security для Windows

Вы можете создать категории приложений для политики Kaspersky Endpoint Security для Windows в папке **Категории приложений** и в окне **Свойства** политики Kaspersky Endpoint Security для Windows.

*Чтобы создать категорию приложений для политики Kaspersky Endpoint Security в папке **Категории приложений**:*

1. В дереве консоли выберите **Дополнительно** → **Управление приложениями** → **Категории приложений**.
2. Нажмите на кнопку **Новая категория** в рабочей области папки **Категории приложений**.

   Запустится мастер создания категории.
3. В окне мастера **Тип категории** выберите тип пользовательской категории:

   - **Пополняемая вручную категория**. Задайте критерии, по которым исполняемые файлы будут попадать в создаваемую категорию.
   - **Пополняемая автоматически категория**. Укажите папку, из которой исполняемые файлы будут автоматически добавлены в созданную категорию.

     При создании категории пополняемой автоматически приложение инвентаризует следующие типы файлов: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX и SCR.
   - **Категория, в которую входят исполняемые файлы с выбранных устройств**. Укажите устройство, исполняемые файлы которого должны попадать в категорию автоматически.
4. Следуйте далее указаниям мастера.

После завершения мастера создается пользовательская категория приложений. Просмотреть созданную категорию можно в списке категорий в рабочей области папки **Категории приложений**.

Если вы хотите экспортировать категорию приложений в файл формата KLC, в контекстном меню категории выберите пункт **Экспортировать**, а затем в открывшемся окне укажите имя файла и нажмите на кнопку **Сохранить**.

Также категорию приложений можно создать в папке **Политики**.

*Чтобы создать категорию приложений в окне **Свойства** политики Kaspersky Endpoint Security для Windows:*

1. В дереве консоли выберите папку **Политики**.
2. В рабочей области папки **Политики** выберите политику Kaspersky Endpoint Security, для которой требуется создать категорию приложений.
3. В контекстном меню выберите пункт **Свойства**.
4. В открывшемся окне **Свойства** в панели **Разделы** выберите раздел **Контроль безопасности** → **Контроль приложений**.

5. В разделе **Контроль приложений** в раскрывающемся списке **Режим Контроля приложений** и **Действие** выберите Список запрещенных или Список разрешенных и нажмите на кнопку **Добавить**.

   Откроется окно **Правило Контроля приложений**, содержащее список категорий.

6. Нажмите на кнопку **Создать**.

7. Введите имя категории и нажмите на кнопку **OK**.

   Запустится мастер создания категории.

8. В окне мастера **Тип категории** выберите тип пользовательской категории:

   - **Пополняемая вручную категория**. Задайте критерии, по которым исполняемые файлы будут попадать в создаваемую категорию.
   - **Пополняемая автоматически категория**. Укажите папку, из которой исполняемые файлы будут автоматически добавлены в созданную категорию.

     При создании категории пополняемой автоматически приложение инвентаризует следующие типы файлов: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX и SCR.

   - **Категория, в которую входят исполняемые файлы с выбранных устройств**. Укажите устройство, исполняемые файлы которого должны попадать в категорию автоматически.

9. Следуйте далее указаниям мастера.

После завершения мастера создается пользовательская категория приложений. Вы можете просмотреть новую категорию в списке категорий приложений.

Категории приложений используются компонентом Контроль приложений, который входит в состав приложения безопасности Kaspersky Endpoint Security для Windows. Компонент Контроль приложений позволяет администратору установить ограничения на запуск приложений на клиентских устройствах, например, на основании приложений, которые входят в выбранную категорию.

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 дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите подпапку **Категории приложений**.

2. Нажмите на кнопку **Новая категория**.

   Запустите мастер **Мастер создания категории**. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На странице мастера **Тип категории** выберите тип пользовательской категории **Пополняемая вручную категория**.

4. На странице мастера **Название категории приложений** введите новое имя категории приложений.

5. На странице **Настройка условий для включения приложений в категории** нажмите на кнопку **Добавить**.

6. В раскрывающемся списке задайте необходимые вам параметры:

- **Из списка исполняемых файлов**

  Если выбран этот вариант, приложения для добавления в категорию можно выбрать из списка исполняемых файлов на клиентском устройстве.

- **Из свойств файла**

  Если выбран этот вариант, можно вручную указать детальные данные исполняемых файлов, которые будут добавлены в пользовательскую категорию программ.

- **Метаданные файлов папки**

  Укажите папку на клиентском устройстве, которая содержит исполняемые файлы. Метаданные исполняемых файлов, входящих в указанную папку, будут передаваться на Сервер администрирования. Исполняемые файлы, имеющие такие же метаданные, будут добавлены в пользовательскую категорию программ.

- **Хеши файлов папки**

  Если выбран этот вариант, можно выбрать или создать папку на клиентском устройстве. Хеш файлов, содержащихся в указанной папке, будет передаваться на Сервер администрирования. Программы, имеющие такой же хеш, как и файлы в указанной папке, будут добавлены в пользовательскую категорию программ.

- **Сертификаты файлов из папки**

  Если выбран этот вариант, можно указать папку на клиентском устройстве, которая содержит исполняемые файлы, подписанные сертификатами. Сертификаты исполняемых файлов считываются и добавляются в условия категории. Исполняемые файлы, подписанные в соответствии с указанными сертификатами, будут добавлены в пользовательскую категорию.

- **Метаданные файлов установщика MSI**

  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.

- **Контрольные суммы файлов msi-инсталлятора приложения**

  Если выбран этот вариант, в качестве условия добавления программ в пользовательскую категорию можно указать файл установщика MSI. Хеш файлов установщика программы будет передаваться на Сервер администрирования. Программы, у которых хеш файлов установщика MSI совпадает с указанным, будут добавлены в пользовательскую категорию программ.

- **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.

- **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**.

- **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).

- **Тип носителя**

  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.

7. На странице мастера **Создание категории приложений** нажмите на кнопку **Готово**.

> Kaspersky Security Center работает с метаданными только из тех файлов, которые содержат цифровую подпись. Невозможно создать категорию на основе метаданных файлов, не содержащих цифровой подписи.

В результате работы мастера будет создана пользовательская категория приложений, пополняемая вручную. Просмотреть созданную категорию можно в списке категорий в рабочей области папки **Категории приложений**.

Если вы хотите экспортировать категорию приложений в файл формата KLC, в контекстном меню категории выберите пункт **Экспортировать**, а затем в открывшемся окне укажите имя файла и нажмите на кнопку **Сохранить**.

Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств

Вы можете использовать исполняемые файлы с устройства как шаблон исполняемых файлов, запуск которых вы хотите разрешить или запретить. На основе исполняемых файлов с выбранных устройств вы можете создать категорию приложений и использовать ее для настройки компонента Контроль приложений.

Чтобы получить список исполняемых файлов с устройств:

1. Убедитесь, что политика Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux создана и активна. Включите в политике компонент Контроль приложений.

2. Получите список исполняемых файлов, хранящихся на клиентских устройствах.

Чтобы создать категорию приложений, в которую входят исполняемые файлы с выбранных устройств:

1. В дереве консоли в папке **Дополнительно → Управление приложениями** выберите подпапку **Категории приложений**.

2. Нажмите на кнопку **Новая категория**.

   Запустите мастер **Мастер создания категории**. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На странице мастера **Тип категории** выберите тип пользовательской категории **Категория приложений, в которую входят исполняемые файлы из выбранных устройств**.

4. На странице мастера **Название категории приложений** введите новое имя категории приложений.

5. На странице мастера **Параметры** нажмите на кнопку **Добавить**.

6. Выберите устройство или устройства, чьи исполняемые файлы будут использоваться для создания категории приложений.

7. Задайте следующие параметры:

   - **Алгоритм вычисления хеш-функции**

     В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky Security Center для файлов категории. Информация о 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 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.

8. На странице мастера **Фильтр** укажите следующие параметры:

   - **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.

9. На странице мастера **Создание категории приложений** нажмите кнопку **Готово**.

После завершения мастера создается пользовательская категория приложений. Просмотреть созданную категорию можно в списке категорий в рабочей области папки **Категории приложений**.

Если вы хотите экспортировать категорию приложений в файл формата KLC, в контекстном меню категории выберите пункт **Экспортировать**, а затем в открывшемся окне укажите имя файла и нажмите на кнопку **Сохранить**.

Создание категории приложений, в которую входят исполняемые файлы из указанных папок

Вы можете использовать исполняемые файлы выбранных папок как эталонный набор исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов из выбранных папок вы можете создать категорию приложений и использовать ее для настройки компонента Контроль приложений.

Чтобы создать категорию приложений, в которую входят исполняемые файлы из указанных папок:

1. В дереве консоли в папке **Дополнительно → Управление приложениями** выберите подпапку **Категории приложений**.

2. Нажмите на кнопку **Новая категория**.

   Запустите мастер **Мастер создания категории**. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На странице мастера **Тип категории** выберите тип пользовательской категории **Категория приложений, в которую входят исполняемые файлы из указанных папок**.

4. На странице мастера **Название категории приложений** введите новое имя категории приложений.

5. На странице мастера **Папка хранилища** нажмите на кнопку **Обзор**.

6. Укажите папку, исполняемые файлы которой будут использоваться для создания категории приложений.

   Максимальная длина полного пути к файлу равна 260 символам.

7. Настройте следующие параметры:

   - **Включать в категорию динамически подключаемые библиотеки (DLL)**

     В категорию приложений включаются динамически подключаемые библиотеки (файлы формата DLL), и компонент Контроль приложений регистрирует действия таких библиотек, запущенных в системе. При включении файлов формата DLL в категорию возможно снижение производительности работы Kaspersky Security Center.

     По умолчанию флажок снят.

   - **Включать в категорию данные о скриптах**

     В категорию приложений включаются данные о скриптах, и скрипты не блокируются компонентом Защита от веб-угроз. При включении данных о скриптах в категорию возможно снижение производительности работы Kaspersky Security Center.

     По умолчанию флажок снят.

   - **Алгоритм вычисления хеш-функции**: **Вычислять SHA256 для файлов в категории (поддерживается для версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)** / **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**

     В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky Security Center для файлов категории. Информация о 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 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.

- **Принудительно проверять папку на наличие изменений**

  Если этот параметр включен, приложение периодически принудительно проверяет папку пополнения категорий на наличие изменений. Периодичность проверки в часах можно указать в поле ввода рядом с флажком. По умолчанию период принудительной проверки равен 24 часам.

  Если этот параметр выключен, принудительная проверка папки не выполняется. Сервер обращается к файлам в папке в случае их изменения, добавления или удаления.

  По умолчанию параметр выключен.

8. На странице мастера **Создание категории приложений** нажмите кнопку **Готово**.

После завершения мастера создается пользовательская категория приложений. Просмотреть созданную категорию можно в списке категорий в рабочей области папки **Категории приложений**.

Если вы хотите экспортировать категорию приложений в файл формата KLC, в контекстном меню категории выберите пункт **Экспортировать**, а затем в открывшемся окне укажите имя файла и нажмите на кнопку **Сохранить**.

Добавление исполняемых файлов, связанных с событием, в категорию приложения

Вы можете добавить исполняемые файлы, связанные с событиями **Запуск приложения запрещен** и **Запуск приложения запрещен в тестовом режиме**, в существующую категорию приложений, пополняемую вручную, или в новую категорию приложений.

Чтобы добавить исполняемые файлы, связанные с событиями компонента Контроль приложений, в категорию приложений:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.

2. В рабочей области узла выберите вкладку **События**.

3. На вкладке **События** выберите нужное вам событие.

4. В контекстном меню события выберите пункт **Добавить в категорию**.

5. В открывшемся окне **Действие с исполняемым файлом, связанным с событием** задайте требуемые параметры:

   Выберите один из следующих вариантов:

   - **Добавить в новую категорию приложений**

     Выберите этот вариант, если необходимо создать новую категорию программ.

     Нажмите на кнопку **ОК**, чтобы запустить мастер создания пользовательской категории. В результате работы мастера будет создана категория с указанными параметрами.

     По умолчанию вариант не выбран.

   - **Добавить в существующую категорию**

     Выберите этот вариант, если необходимо добавить правила в существующую категорию программ. Выберите необходимую категорию в списке категорий программ.

     По умолчанию этот вариант выбран.

   В блоке **Тип правила** выберите параметры:

   - **Добавить в категорию**

     Выберите этот вариант, если необходимо добавить правила в условия категории программ.

     По умолчанию этот вариант выбран.

   - **Правила для добавления в исключения**

     Выберите этот вариант, если необходимо добавить правила в исключения категории программ.

   В блоке **Тип информации о файле** выберите один из параметров:

   - **Certificate details (or SHA256 hashes for files without certificate)**

     Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одного приложения могут быть подписаны одним сертификатом или несколько разных приложений одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий приложения или несколько приложений одного производителя.

     Каждый файл имеет свою уникальную хеш-функцию SHA256. При выборе хеш-функции SHA256 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

     Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла или хеш-функцию SHA256 для файлов без сертификата.

     По умолчанию выбран этот вариант.

   - **Данные сертификата (файлы без сертификата пропускаются)**

     Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одного приложения могут быть подписаны одним сертификатом или несколько разных приложений одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий приложения или несколько приложений одного производителя.

Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла. Если у исполняемого файла нет сертификата, то такой файл будет пропущен. Информация о нем не будет добавлена в категорию.

- **Только SHA256 (файлы без хеша пропускаются)**

  Каждый файл имеет свою уникальную хеш-функцию SHA256. При выборе хеш-функции SHA256 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

  Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции SHA256 исполняемого файла.

- **MD5 (устаревший режим, только для версий Kaspersky Endpoint Security 10 Service Pack 1)**

  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.

6. Нажмите на кнопку **OK**.

Настройка управления запуском приложений на клиентских устройствах

Категоризация приложений позволяет оптимизировать процесс управления запуском приложений на устройствах. Вы можете создать категорию приложений и настроить компонент Контроль приложений политики так, что на устройствах, на которых применена эта политика, будут запускаться только приложения из указанной категории. Например, вы создали категорию, которая содержит приложения *Приложение_1* и *Приложение_2*. После добавления этой категории в политику, на устройствах, к которым применена эта политика, будет разрешен запуск только двух приложений, *Приложение_1* и *Приложение_2*. Если пользователь попытается запустить приложение, которое не входит в категорию, например, *Приложение_3*, то запуск такого приложения будет заблокирован. Пользователю будет отображено сообщение о том, что запуск *Приложения_3* запрещен в соответствии с правилом Контроля приложений. Вы можете создать автоматически пополняемую категорию на основе различных критериев, входящих в указанную папку. В этом случае файлы будут автоматически добавляться в категорию из указанной папки. Исполняемые файлы приложений копируются в указанную папку, обрабатываются автоматически, и их метрики заносятся в категорию.

Чтобы настроить управление запуском приложений на клиентских устройствах:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Категории приложений**.

2. В рабочей области папки **Категории приложений** создайте категории приложений, запуском которых вы хотите управлять.

3. Чтобы создать политику для приложения Kaspersky Endpoint Security для Windows, в папке **Управляемые устройства** на вкладке **Политики** нажмите на кнопку **Новая политика** и следуйте указаниям мастера.

   Если такая политика уже существует, этот шаг можно пропустить. Управление запуском приложений в указанной категории можно настроить в параметрах этой политики. Созданная политика отображается в папке **Управляемые устройства** на вкладке **Политики**.

4. В контекстном меню политики для приложения Kaspersky Endpoint Security для Windows выберите пункт **Свойства**.

   Откроется окно свойств политики Kaspersky Endpoint Security для Windows.

5. В окне свойств политики Kaspersky Endpoint Security для Windows, в разделе **Контроль безопасности** → **Контроль приложений** установите флажок **Контроль приложений**.

6. Нажмите на кнопку **Добавить**.

   Откроется окно **Правило Контроля приложений**.

7. В окне **Правило Контроля приложений** в раскрывающемся списке **Категория** выберите категорию приложений, на которую будет распространяться правило запуска. Настройте параметры правила запуска для выбранной категории приложений.

   Для приложений версий Kaspersky Endpoint Security для Windows 10 Service Pack 2 и выше категории, созданные по критерию MD5-хеша исполняемого файла, приложения не отображаются.

   Не рекомендуется добавлять категорию, созданную по критерию SHA256 исполняемого файла, для версий приложений ниже Kaspersky Endpoint Security 10 Service Pack 2. Это может привести к сбою приложения.

   Подробные инструкции по настройке правил контроля приведены в справке Kaspersky Endpoint Security для Windows.

8. Нажмите на кнопку **OK**.

Запуск приложений на устройствах, входящих в указанную категорию, будет выполняться согласно созданному правилу. Созданное правило отображается в окне свойств политики Kaspersky Endpoint Security для Windows в разделе **Контроль приложений**.

Просмотр результатов статического анализа правил запуска исполняемых файлов

Чтобы просмотреть информацию о том, запуск каких исполняемых файлов запрещен пользователям:

1. В дереве консоли в папке **Управляемые устройства** выберите вложенную папку **Политики**.

2. В контекстном меню политики для приложения Kaspersky Endpoint Security для Windows выберите пункт **Свойства**.

   Откроется окно свойств политики приложения.

3. В окне свойств политики в панели **Разделы** выберите раздел **Контроль безопасности**, а затем подраздел **Контроль приложений**.

4. Нажмите на кнопку **Статический анализ**.

   Откроется окно **Анализ списка прав доступа**. В левой части окна отображается список пользователей, основанный на данных Active Directory.

5. Выберите в списке пользователя.

   В правой части окна отобразятся категории приложений, назначенные этому пользователю.

6. Чтобы просмотреть исполняемые файлы, запуск которых запрещен пользователю, в окне **Анализ списка прав доступа** нажмите на кнопку **Просмотреть файлы**.

   Откроется окно, в котором отображается список исполняемых файлов, запуск которых запрещен пользователю.

7. Чтобы просмотреть список исполняемых файлов, входящих в категорию, выберите категорию приложений и нажмите на кнопку **Просмотреть файлы категории**.

   В открывшемся окне отображается список исполняемых файлов, входящих в категорию приложений.

Просмотр реестра приложений

Kaspersky Security Center выполняет инвентаризацию программного обеспечения, установленного на управляемых устройствах.

Агент администрирования составляет список приложений, установленных на устройстве с операционной системой Windows или Linux, и передает список Серверу администрирования. 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 реестр установленных на клиентских устройствах приложений,

В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Реестр приложений**.

В рабочей области папки **Реестр приложений** отображается список приложений, установленных на клиентских устройствах и Сервере администрирования.

Вы можете просмотреть подробную информацию о любом приложении, выбрав в контекстном меню этого приложения пункт **Свойства**. В окне свойств приложения отображается общая информация о приложении и информация об исполняемых файлах приложения, а также список устройств, на которых установлено приложение.

В контекстном меню любого приложения вы можете:

- добавить это приложение в категорию приложений;
- назначить тег приложению;
- экспортировать список приложений в файлы форматов CSV или TXT;
- просмотреть свойства 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.

Для просмотра приложений, удовлетворяющих определенным критериям, вы можете воспользоваться полями фильтрации в рабочей области папки **Реестр приложений**.

В окне свойств выбранного устройства в разделе **Реестр приложений** вы можете просмотреть список приложений, установленных на устройстве.

Генерирование отчета об установленных приложениях

В рабочей области папки **Реестр приложений** вы также можете нажать на кнопку **Просмотреть отчет об установленных приложениях**, чтобы сгенерировать отчет, содержащий информацию об установленных приложениях, включая количество устройств, на которых установлено каждое приложение. Отчет, который открывается на странице **Отчет об установленных приложениях**, содержит информацию о приложениях "Лаборатории Касперского" и о приложениях сторонних производителей. Если вам нужна информация только о приложениях "Лаборатории Касперского", установленных на клиентских устройствах, в списке **Сводная информация** выберите "Лаборатория Касперского".

Информация о приложениях "Лаборатории Касперского" и других производителей на устройствах, подключенных к подчиненным и виртуальным Серверам администрирования, также хранится в реестре приложений главного Сервера администрирования. После добавления данных с подчиненных и виртуальных Серверов нажмите на кнопку **Просмотреть отчет об установленных приложениях**, и на открывшейся странице **Отчет об установленных приложениях** вы можете просмотреть эту информацию.

Чтобы добавить информацию с подчиненных и виртуальных Серверов администрирования в отчет об установленных приложениях:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. На вкладке **Отчеты** выберите **Отчет об установленных приложениях**.
4. В контекстном меню отчета выберите пункт **Свойства**.

   Откроется окно **Свойства: Отчет об установленных приложениях**.
5. В разделе **Иерархия Серверов администрирования** установите флажок **Включать данные подчиненных и виртуальных Серверов администрирования**.
6. Нажмите на кнопку **ОК**.

В результате информация с подчиненных и виртуальных Серверов администрирования будет включена в **Отчет об установленных приложениях**.

Изменение времени начала инвентаризации программного обеспечения

Kaspersky Security Center выполняет инвентаризацию программного обеспечения, установленного на управляемых клиентских устройствах, работающих под управлением операционной системы Windows.

Агент администрирования составляет список приложений, установленных на устройстве, и передает список Серверу администрирования. Агент администрирования автоматически получает информацию об установленных приложениях из реестра Windows.

Чтобы сохранить ресурсы устройства, по умолчанию Агент администрирования начинает получать информацию об установленных приложениях через 10 минут после запуска службы Агента администрирования.

Чтобы изменить время начала инвентаризации программного обеспечения устройства после запуска службы Агента администрирования:

1. Откройте системный реестр устройства, на котором установлен Агент администрирования, например, локально с помощью команды regedit в меню **Пуск → Выполнить**.
2. Перейдите в раздел:
   - для 32-разрядной системы:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
   - для 64-разрядной системы:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentF
3. Для ключа KLINV_INV_COLLECTOR_START_DELAY_SEC установите нужное вам значение в секундах.
   По умолчанию указано значение 600 секунд.
4. Перезапустите службу Агента администрирования.

В результате время начала инвентаризации программного обеспечения после запуска службы Агента администрирования изменится.

Окно Информация о группе лицензионных программ

В этом окне можно задать критерии включения обнаруженных программ в группу лицензионных программ.

Название группы лицензионных программ

Название создаваемой группы лицензионных программ.

Отслеживать нарушение ограничений

Если флажок установлен, при нарушении указанных ограничений ключа группы лицензионных программ на Сервере администрирования регистрируется информационное событие.

По умолчанию флажок установлен.

Критерии включения обнаруженных программ в эту группу лицензионных программ

В поле отображаются критерии включения программ, установленных на клиентских устройствах, в создаваемую группу лицензионных программ.

Добавить

При нажатии на кнопку открывается окно **Информация о группе лицензионных программ**, в котором можно задать критерии включения программ в создаваемую группу лицензионных программ.

Просмотреть подходящие программы

При нажатии на кнопку открывается окно **Программы**, в котором отображаются программы, соответствующие заданным критериям. Окно открывается, если задан хотя бы один критерий.

Создание групп лицензионных приложений

Чтобы создать группу лицензионных приложений:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Учет сторонних лицензий**.

2. По кнопке **Добавить группу лицензионных приложений** запустите Мастер добавления группы лицензионных приложений.

   Запускается Мастер добавления группы лицензионных приложений.

3. На шаге **Информация о группе лицензионных приложений** укажите, какие приложения вы хотите включить в группу приложений:

   - **Название группы лицензионных приложений**

   - **Отслеживать нарушение ограничений**

     При нарушении одного из ограничений, которые вы накладываете на лицензионный ключ группы приложений, Сервер администрирования регистрирует событие информационное, предупреждающее или отказ функционирования:

     - Информационное событие: **Для одной из групп лицензионных приложений число разрешенных установок исчерпано более чем на 95%**.

     - Предупреждающее событие: **Для одной из групп лицензионных приложений скоро будет превышено ограничение числа установок**.

     - Отказ функционирования: **Для одной из групп лицензионных приложений превышено ограничение числа установок**.

       Событие регистрируется только один раз при выполнении условия. В следующий раз это же событие может быть зарегистрировано только тогда, когда количество установок вернется к нормальному уровню, а затем событие произойдет снова. Событие не может быть зарегистрировано чаще одного раза в час.

   - **Критерии включения обнаруженных приложений в эту группу лицензионных приложений**

     Укажите критерии, чтобы определить, какие приложения вы хотите включить в группу приложений. Вы можете определять приложения по имени приложения, версии приложения, поставщику и тегу. Вам нужно указать хотя бы один критерий. Приложение добавляется в группу, если выполняется хотя бы один из критериев.

4. На шаге **Введите данные о имеющихся лицензионных ключах** укажите лицензионные ключи, которые вы хотите отслеживать. Выберите параметр **Контролировать нарушение заданных лицензионных ограничений** и добавьте лицензионные ключи:

   a. Нажмите на кнопку **Добавить**.

   b. Выберите лицензионный ключ, который нужно добавить, и нажмите на кнопку **ОК**. Если необходимый лицензионный ключ отсутствует в списке, нажмите на кнопку **Добавить** и укажите свойства лицензионного ключа.

5. На шаге **Добавление группы лицензионных приложений** нажмите на кнопку **Готово**.

Группа лицензионных приложений создана и отображается в папке **Учет сторонних лицензий**.

Управление лицензионными ключами для групп лицензионных приложений

Чтобы создать лицензионный ключ для группы лицензионных приложений:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Учет сторонних лицензий**.

2. Нажмите на кнопку **Управлять лицензионными ключами лицензионных приложений** в рабочей области папки **Учет сторонних лицензий**.

   Откроется окно **Управление лицензионными ключами лицензионных приложений**.

3. В окне **Управление лицензионными ключами лицензионных приложений** нажмите на кнопку **Добавить**.

   Откроется окно **Лицензионный ключ**.

4. В окне **Лицензионный ключ** укажите свойства лицензионного ключа и ограничения, которые этот лицензионный ключ накладывает на группу лицензионных приложений.

   - **Название**. Название лицензионного ключа.
   - **Комментарий**. Примечания к выбранному лицензионному ключу.
   - **Ограничение**. Количество устройств, на которых может быть установлено приложение, использующее этот лицензионный ключ.
   - **Действителен до**. Дата окончания срока действия лицензионного ключа.

Созданные лицензионные ключи отображаются в окне **Управление лицензионными ключами лицензионных приложений**.

Чтобы применить лицензионный ключ к группе лицензионных приложений:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Учет сторонних лицензий**.

2. В папке **Учет сторонних лицензий** выберите группу лицензионных приложений, к которой вы хотите применить лицензионный ключ.

3. В контекстном меню группы лицензионных приложений выберите пункт **Свойства**.

   Откроется окно свойств группы лицензионных приложений.

4. В окне свойств группы лицензионных приложений в разделе **Лицензионные ключи** выберите вариант **Контролировать нарушение заданных лицензионных ограничений**.

5. Нажмите на кнопку **Добавить**.

   Откроется окно **Выбор лицензионного ключа**.

6. В окне **Выбор лицензионного ключа** выберите лицензионный ключ, который вы хотите применить к группе лицензионных приложений.

7. Нажмите на кнопку **OK**.

Ограничения для группы лицензионных приложений, указанные в лицензионном ключе, будут распространены на выбранную группу лицензионных приложений.

Инвентаризация исполняемых файлов

Вы можете получить список исполняемых файлов, хранящихся на управляемых устройствах. Для инвентаризации исполняемых файлов вам нужно создать задачу инвентаризации.

Функция инвентаризации исполняемых файлов доступна для следующих приложений:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux
- Kaspersky Security для виртуальных сред 4.0 Легкий агент и выше

Количество исполняемых файлов, получаемых от одного устройства, не может превышать 150 000. При достижении этого ограничения Kaspersky Security Center не получит новые файлы.

Прежде чем начать, включите уведомления о запуске приложений в политике Kaspersky Endpoint Security и в политике Агента администрирования, чтобы можно было передавать данные на Сервер администрирования.

Чтобы включить уведомления о запуске приложения:

- Откройте параметры политики Kaspersky Endpoint Security и выполните следующие действия:
  1. Перейти к **Общие параметры** → **Отчеты и хранилища**.
  2. В разделе **Передача данных на Сервер администрирования**, установите флажок **О запускаемых приложениях**.
  3. Сохраните изменения.
- Откройте параметры политики Агента администрирования и выполните следующие действия:
  1. Перейти в раздел **Хранилища**.
  2. Установите флажок **Информация об установленных приложениях**.
  3. Сохраните изменения.

Чтобы создать задачу инвентаризации исполняемых файлов на клиентских устройствах:

1. В дереве консоли выберите папку **Задачи**.
2. В рабочей области папки **Задачи** нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи.

3. В окне мастера **Выбор типа задачи** выберите тип задачи **Kaspersky Endpoint Security**, затем подтип задачи **Инвентаризация** и нажмите на кнопку **Далее**.

4. Следуйте дальнейшим шагам мастера.

   В результате работы мастера создается задача инвентаризации для Kaspersky Endpoint Security. Созданная задача отображается в списке задач в рабочей области папки **Задачи**.

Список исполняемых файлов, обнаруженных на устройствах в результате выполнения инвентаризации, отображается в рабочей области папки **Исполняемые файлы**.

При выполнении инвентаризации приложение обнаруживает исполняемые файлы следующих форматов: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, а также HTML-файлы.

Просмотр информации об исполняемых файлах

Чтобы просмотреть список всех исполняемых файлов, обнаруженных на клиентских устройствах,

В дереве консоли в папке **Управление приложениями** выберите вложенную папку **Исполняемые файлы**.

В рабочей области папки **Исполняемые файлы** отображается список исполняемых файлов, которые запускались на устройствах или были обнаружены в процессе работы задачи инвентаризации Kaspersky Endpoint Security для Windows.

Для просмотра данных об исполняемых файлах, удовлетворяющих определенным критериям, вы можете воспользоваться фильтрацией.

Чтобы просмотреть свойства исполняемого файла,

в контекстном меню файла выберите пункт **Свойства**.

Откроется окно, содержащее информацию об исполняемом файле, а также список устройств, на которых присутствует исполняемый файл.

Мониторинг и отчеты

В этом разделе описаны функции мониторинга и работа с отчетами в Kaspersky Security Center. Эти функции позволяют получать сведения об инфраструктуре вашей сети, статусе защиты, а также статистику.

В процессе развертывания или во время работы Kaspersky Security Center можно настраивать функции мониторинга и параметры отчетов.

- **Индикаторы**

  В Консоли администрирования можно быстро оценить текущее состояние Kaspersky Security Center и управляемых устройств с помощью цветовых индикаторов.

- **Статистика**

  Статистическая информация о состоянии системы защиты и управляемых устройств отображается в виде настраиваемых информационных панелей.

- **Reports**

  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.

- **События**

  Выборки событий предназначены для просмотра на экране именованных наборов событий, которые выбраны из базы данных Сервера администрирования. Эти типы событий сгруппированы по следующим категориям:

  - Уровень важности: **Критические события**, **Отказы функционирования**, **Предупреждения** и **Информационные события**.
  - Время: **Последние события**.
  - Тип: **Запросы пользователей** и **События аудита**.

Вы можете создавать и просматривать определенные пользователем выборки событий на основе параметров, доступных для настройки в интерфейсе Kaspersky Security Center Web Console.

Сценарий: мониторинг и отчеты

В этом разделе представлен сценарий настройки мониторинга и отчетов в Kaspersky Security Center.

Предварительные требования

После развертывания Kaspersky Security Center в сети организации вы можете приступить к мониторингу состояния безопасности сети с помощью Kaspersky Security Center и к формированию отчетов.

Этапы

Мониторинг и работа с отчетами в сети организации состоят из следующих этапов:

1. **Настройка переключения статусов устройств**

   Ознакомьтесь с параметрами, определяющими присвоение статусов устройствам в зависимости от конкретных условий. Изменяя эти параметры, вы можете изменить количество событий с уровнями важности *Критический* или *Предупреждение*.

   При настройке переключения статусов устройств убедитесь, что новые параметры не конфликтуют с политиками информационной безопасности вашей организации и что вы можете своевременно реагировать на важные события безопасности в сети вашей организации.

2. **Настройка параметров уведомлений о событиях на клиентских устройствах**

   Настройте уведомления (по электронной почте, по SMS или с помощью запуска исполняемого файла) о событиях на клиентских устройствах, в соответствии с потребностями вашей организации.

3. **Изменение ответа вашей сети безопасности на событие Вирусная атака**

   Чтобы настроить ответ сети на новые события, 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. **Работа со статистической информацией**

   Настройте отображение статистики в соответствии с потребностями вашей организации.

5. **Просмотр состояния безопасности сети вашей организации**

   Чтобы проверить состояние безопасности сети вашей организации, вы можете выполнить любое из следующих действий:

   - В рабочей области узла **Сервер администрирования**, на вкладке **Статистика** откройте вкладку второго уровня (страницу) **Состояние защиты** и просмотрите информационную панель **Статус постоянной защиты**.
   - Генерация и просмотр отчета **Отчет о состоянии защиты**.
   - Генерация и просмотр отчета **Отчет об ошибках**.

6. **Нахождение незащищенных клиентских устройств**

   Чтобы найти незащищенные клиентские устройства, перейдите в рабочую область узла **Сервер администрирования**, на вкладке **Статистика** откройте вкладку второго уровня (страницу) **Состояние защиты** и просмотрите информационную панель **История обнаружения новых устройств в сети**. Также можно создать и просмотреть **Отчет о развертывании защиты**.

7. **Проверка защиты клиентских устройств**

   Чтобы проверить защиту клиентских устройств, перейдите в рабочую область узла **Сервер администрирования**, на вкладке **Статистика** откройте вкладку второго уровня (страницу) **Развертывание** или **Статистика угроз** и просмотрите соответствующие информационные панели. Вы также можете начать и просматривать выборку событий **Критические события**.

8. **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.

   Чтобы оценить загрузку событий в базе данных, рассчитайте место в базе данных. Вы также можете ограничить максимальное количество событий чтобы избежать переполнения базы данных.

9. **Просмотр информации о лицензии**

   Чтобы просмотреть информацию о лицензии, перейдите в рабочую область узла **Сервер администрирования**, на вкладке **Статистика** откройте вкладку второго уровня (страницу) **Развертывание** и просмотрите информационную панель **Использование лицензионных ключей**. Также можно создать и просмотреть **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.

Мониторинг цветовых индикаторов и зарегистрированных событий в Консоли администрирования

В Консоли администрирования можно быстро оценить текущее состояние Kaspersky Security Center и управляемых устройств с помощью цветовых индикаторов. Индикаторы отображаются в рабочей области узла **Сервер администрирования** на вкладке **Мониторинг**. На вкладке есть шесть информационных блоков с цветовыми индикаторами и зарегистрированными событиями. Цветной индикатор – это цветная вертикальная полоса на левой стороне панели. Каждый блок с индикатором отвечает за отдельную функциональную область Kaspersky Security Center (см. таблицу ниже).

Области ответственности цветовых индикаторов в Консоли администрирования

Название панели	Область ответственности цветового индикатора
Развертывание	Установка Агента администрирования и приложений безопасности на устройства сети организации.
Структура управления	Структура групп администрирования. Сканирование сети. Правила перемещения устройств.
Настройка защиты	Функции приложения безопасности: состояние защиты, поиск вредоносного ПО.
Обновление	Обновления и патчи.
Мониторинг	Состояние защиты.
Сервер администрирования	Функции и свойства Сервера администрирования.

Индикатор может быть одного из пяти цветов (см. таблицу ниже). Цвет индикатора зависит от текущего состояния Kaspersky Security Center и от зарегистрированных событий.

Цветовые кодировки индикаторов

Состояние	Цвет индикатора	Значение цвета индикатора
Информационное	Зеленый	Вмешательство администратора не требуется.
Предупреждение	Желтый	Требуется вмешательство администратора.
Предельный	Красный	Имеются серьезные проблемы. Требуется вмешательство администратора для их решения.
Информационное	Голубой	Зарегистрированы события, не связанные с угрозами для безопасности управляемых устройств.
Информационное	Серый	Информация о событиях недоступна или еще не получена.

Цель администратора – поддерживать индикаторы в состоянии "зеленый" на всех информационных панелях вкладки **Мониторинг**.

На информационных панелях также отображаются зарегистрированные события, влияющие на цветовые индикаторы, и состояние Kaspersky Security Center (см. таблицу ниже).

Название, описание и цвет индикатора зарегистрированных событий

Цвет индикатора	Отображаемое имя типа события	Тип события	Описание
Красный	**Количество устройств, на которых срок действия лицензии истек: %1**	IDS_AK_STATUS_LIC_EXPAIRED	События этого типа возникают, если срок действия коммерческой лицензии окончен. Один раз в день Kaspersky Security Center проверяет, не истек ли срок действия лицензии. После окончания срока действия коммерческой лицензии, Kaspersky Security Center работает в режиме Базовой функциональности. Чтобы продолжить использование Kaspersky Security Center, продлите срок действия коммерческой лицензии.

Цвет индикатора	Отображаемое имя типа события	Тип события	Описание
Красный	**Устройств с не запущенным приложением безопасности: %1**	IDS_AK_STATUS_AV_NOT_RUNNING	События этого типа возникают, когда приложение безопасности, установленное на устройстве, не запущено. Убедитесь, что на устройстве запущено приложение Kaspersky Endpoint Security.
Красный	**Устройств с выключенной защитой: %1**	IDS_AK_STATUS_RTP_NOT_RUNNING	События такого типа возникают, когда приложение защиты на устройстве отключено больше указанного времени. Проверьте текущий статус постоянной защиты на устройстве и убедитесь, что все необходимые вам компоненты защиты включены.
Красный	**Обнаружена уязвимость в программном обеспечении на устройствах**	IDS_AK_STATUS_VULNERABILITIES_FOUND	События этого типа происходят, когда задача *Поиск уязвимостей и требуемых обновлений* обнаружила уязвимости с указанным уровнем критичности в приложениях, установленных на устройстве. Проверьте список доступных обновлений в подпапке **Обновления программного обеспечения**, вложенной в папку **Управление приложениями**. Эта папка содержит список полученных Сервером администрирования обновлений приложений Microsoft и других производителей программного обеспечения, которые могут быть распространены на устройства. Просмотрите информацию о доступных обновлениях и установите их на устройство.
Красный	**На Сервере администрирования зарегистрированы критические события**	IDS_AK_STATUS_EVENTS_OCCURED	События этого типа возникают при обнаружении критических событий Сервера администрирования. Проверьте список событий, хранящихся на Сервере администрирования, а затем последовательно исправьте критические события.
Красный	**На Сервере администрирования зарегистрированы ошибки в событиях**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	События этого типа возникают при регистрации непредвиденных ошибок на стороне Сервера администрирования. Проверьте список событий, хранящихся на Сервере администрирования, а затем последовательно исправьте критические события.
Красный	**Потеряно соединение с устройствами: %1**	IDS_AK_STATUS_ADM_LOST_CONTROL1	События этого типа возникают при потере соединения между Сервером администрирования и устройством. Просмотрите список отключенных устройств и попробуйте подключить их снова.
Красный	**Устройств, которые давно не соединялись с Сервером администрирования: %1**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	События этого типа возникают, когда устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено. Убедитесь, что устройство включено и запущен Агент администрирования.
Красный	**Устройств со статусом отличным от "OK": %1**	IDS_AK_STATUS_HOST_NOT_OK	События этого типа происходят, когда статус устройства *OK*, подключенного к Серверу администрирования, меняется на *Критический* или *Предупреждение*. Устранить неполадку можно с помощью утилиты удаленной диагностики Kaspersky Security Center.

Цвет индикатора	Отображаемое имя типа события	Тип события	Описание
Красный	**Базы устарели: %1 устройств**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	События этого типа возникают, когда антивирусные базы на устройстве не обновлялись в течение заданного интервала времени. Следуйте инструкциям, чтобы обновить антивирусные базы "Лаборатории Касперского".
Красный	**Устройств, на которых давно не осуществлялась проверка обновлений Центра обновления Windows: %1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	События этого типа возникают, когда задача *Синхронизация обновлений Windows Update* не выполнялась больше указанного времени. Следуйте инструкциям, чтобы синхронизировать обновления из Центра обновления Windows Update с Сервером администрирования.
Красный	**Для Kaspersky Security Center требуется установка плагинов: %1**	IDS_AK_STATUS_PLUGINS_REQUIRED2	События этого типа возникают, когда вам нужно установить дополнительные плагины для приложений "Лаборатории Касперского". Загрузите и установите необходимые плагины управления для приложения "Лаборатории Касперского" с веб-сайта Службы технической поддержки "Лаборатории Касперского".

Работа с отчетами, статистикой и уведомлениями

В этом разделе представлена информация о работе с отчетами, статистикой и выборками событий и устройств в Kaspersky Security Center, а также о настройке параметров уведомлений Сервера администрирования.

Работа с отчетами

Отчеты в Kaspersky Security Center содержат информацию о состоянии управляемых устройств. Отчеты формируются на основании информации, хранящейся на Сервере администрирования. Вы можете создавать отчеты для следующих объектов:

- для выборок устройств, созданных по определенным параметрам;
- для групп администрирования;
- для наборов устройств из разных групп администрирования;
- для всех устройств в сети (в отчете о развертывании).

В приложении есть набор стандартных шаблонов отчетов. Предусмотрена также возможность создавать пользовательские шаблоны отчетов. Отчеты отображаются в главном окне приложения, в папке дерева консоли **Сервер администрирования**.

Создание шаблона отчета

Чтобы создать шаблон отчета:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. Нажмите на кнопку **Новый шаблон отчета**.

   В результате запустится мастер создания шаблона отчета. Следуйте далее указаниям мастера.

После окончания работы мастера сформированный шаблон отчета будет добавлен в состав выбранной папки **Сервер администрирования** дерева консоли. Этот шаблон можно использовать для создания 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 дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. В списке шаблонов отчетов выберите требуемый шаблон отчета.
4. В контекстном меню выбранного шаблона отчета выберите пункт **Свойства**.

   В качестве альтернативы, можно сначала сформировать отчет, а затем нажать на кнопку **Открыть свойства шаблона отчета** или **Настроить столбцы отчета**.

5. В открывшемся окне вы можете изменить свойства шаблона отчета. Свойства каждого отчета могут содержать только некоторые из разделов, описанных ниже.

   - Раздел **Общие**:

     - Название шаблона отчета
     - **Максимальное число отображаемых записей**

       Если этот параметр включен, количество отображаемых в таблице записей с подробными данными отчета не превышает указанное значение.

       Записи отчета сначала сортируются в соответствии с правилами, указанными в разделе **Столбцы → 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.

- **Версия для печати**

  Отчет оптимизирован для печати: добавлены пробелы, между некоторыми значениями для лучшей визуальной доступности.

  По умолчанию параметр включен.

- Раздел **Столбцы**.

  Выберите поля, которые будут отображаться в отчете и порядок этих полей. Также настройте, должна ли информация в отчете сортироваться и фильтроваться по каждому из полей.

- Раздел **Период**.

  Измените отчетный период. 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.

- Разделы **Группа**, **Выборка устройств**, или **Устройства**.

  Измените набор клиентских устройств, для которых создается отчет. В зависимости от параметров, указанных при создании шаблона, может присутствовать только один из этих разделов.

- Раздел **Параметры**.

  Измените параметры отчета. Набор параметров зависит от конкретного отчета.

- Раздел **Безопасность**. **Наследовать параметры Сервера администрирования**

  Если этот параметр включен, параметры отчета наследуются с Сервера администрирования.

  Если этот параметр выключен, вы можете настроить параметры отчета. Вы можете назначить роль пользователю или группе пользователей или назначить права пользователю или группе пользователей, применительно к отчету.

  По умолчанию параметр включен.

  > Раздел **Безопасность** доступен, если в окне параметров интерфейса установлен флажок **Отображать разделы с параметрами безопасности**.

- Раздел **Иерархия Серверов администрирования**:

  - **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 **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.

Расширенный формат фильтра в шаблонах отчета

В приложении Kaspersky Security Center 15.1 вы можете применить расширенный формат фильтра к шаблону отчета. Расширенный формат фильтра обеспечивает большую гибкость по сравнению с форматом по умолчанию. Вы можете создавать сложные условия фильтрации, используя набор фильтров, которые будут применяться к отчету с помощью логического оператора OR при создании отчета, как показано ниже:

Фильтр[1](Поле[1] AND Поле[2]... AND Поле[n]) OR Фильтр[2](Поле[1] AND Поле[2]... AND Поле[n]) OR... Фильтр[n](Поле[1] AND Поле[2]... AND Поле[n])

Кроме того, с помощью расширенного формата фильтра вы можете установить значение временного интервала в формате относительного времени (например, с помощью условия "За последние N дней") для определенных полей фильтра. Доступность и набор условий временного интервала зависят от типа шаблона отчета.

Конвертация фильтра в расширенный формат

Расширенный формат фильтра для шаблонов отчета поддерживается только в версии Kaspersky Security Center 12 и выше. После конвертации фильтра по умолчанию в расширенный формат, шаблон отчета становится несовместимым с Серверами администрирования вашей сети, на которых установлены более ранние версии Kaspersky Security Center. Информация с этих Серверов администрирования не будет получена для отчета.

Чтобы конвертировать из формата по умолчанию в расширенный формат:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. В списке шаблонов отчетов выберите требуемый шаблон отчета.
4. В контекстном меню выбранного шаблона отчета выберите пункт **Свойства**.
5. В отобразившемся окне свойств выберите раздел **Столбцы**.
6. На вкладке **Детальные данные** перейдите по ссылке **Конвертировать фильтр**.
7. В появившемся окне нажмите на кнопку **OK**.

   Конвертация в расширенный формат фильтра необратима для шаблона отчета, к которому он применяется. Если вы случайно перешли по ссылке **Конвертировать фильтр**, вы можете отменить изменения, нажав на кнопку **Отмена** в окне свойств шаблона отчета.

8. Чтобы применить изменения, закройте окно свойств шаблона отчета, нажав на кнопку **OK**.

   Когда снова откроется окно свойств шаблона отчета, отобразится новый доступный раздел **Фильтры**. В этом разделе вы можете настроить расширенный формат фильтра.

Настройка расширенного фильтра

Чтобы настроить параметры расширенного фильтра в шаблоне отчета:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. В списке шаблонов отчетов выберите шаблон отчета, который ранее был конвертирован в расширенный формат фильтра.
4. В контекстном меню выбранного шаблона отчета выберите пункт **Свойства**.
5. В отобразившемся окне свойств выберите раздел **Фильтры**.

   Раздел **Фильтры** не отображается, если шаблон отчета не был сконвертирован в расширенный формат фильтра.

   В окне свойства шаблона отчета в разделе **Фильтры** вы можете просмотреть и изменить список примененных фильтров к отчету. Каждый фильтр в списке имеет уникальное имя и представляет собой набор фильтров для соответствующих полей в отчете.
6. Откройте окно свойств фильтра одним из следующих способов:

   - Чтобы создать фильтр, нажмите на кнопку **Добавить**.
   - Чтобы изменить существующий фильтр, выберите необходимый фильтр и нажмите на кнопку **Изменить**.
7. В открывшемся окне выберите и укажите значения обязательных полей фильтра.
8. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно.

   Если вы создаете фильтр, имя фильтра должно быть указано в поле **Имя фильтра**, прежде чем нажать на кнопку **ОК**.
9. Закройте окно свойств шаблона отчета, нажав на кнопку **ОК**.

   Расширенный фильтр в шаблоне отчета настроен. Теперь вы можете создавать отчеты используя это шаблон отчета.

Создание и просмотр отчета

Чтобы сформировать и просмотреть отчет:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. Выберите интересующий вас шаблон отчета в списке шаблонов двойным нажатием клавиши мыши.

   Отобразится выбранный шаблон отчета.

В отчете отображаются следующие данные:

- 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;
- таблица с детальными данными отчета.

Сохранение отчета

Чтобы сохранить сформированный отчет:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. Выберите интересующий вас шаблон отчета в списке шаблонов.
4. В контекстном меню выбранного шаблона отчета выберите пункт **Сохранить**.

   В результате запустится мастер сохранения отчета. Следуйте далее указаниям мастера.

После завершения работы мастера откроется папка, в которую вы сохранили файл отчета.

Когда вы сохраняете отчет в виде файла XLS, все связанные изображения, такие как логотип и датаграмма, сохраняются как отдельные файлы.

Создание задачи рассылки отчета

Отчеты можно рассылать по электронной почте. Рассылка отчетов в Kaspersky Security Center осуществляется с помощью задачи рассылки отчета.

Чтобы создать задачу рассылки одного отчета:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. Выберите интересующий вас шаблон отчета в списке шаблонов.
4. В контекстном меню выбранного шаблона отчета выберите пункт **Рассылка отчетов**.

   В результате запускается мастер создания задачи рассылки выбранного отчета. Следуйте далее указаниям мастера.

Чтобы создать задачу рассылки нескольких отчетов:

1. В дереве консоли в узле с именем нужного вам Сервера администрирования выберите папку **Задачи**.
2. Нажмите на кнопку **Создать задачу** в рабочей области папки **Задачи**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

Созданная задача рассылки отчета отображается в папке дерева консоли **Задачи**.

Задача рассылки отчета создается автоматически в случае, если при установке Kaspersky Security Center были заданы параметры электронной почты.

Шаг 1. Выбор типа задачи

В окне **Выбор типа задачи** в списке задач выберите тип задачи **Рассылка отчетов**.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 2. Выбор типа отчета

В окне **Выбор типа отчета** в списке шаблонов для создания задачи выберите тип отчета.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 3. Действия над отчетом

В разделе **Действия с отчетами** укажите следующие параметры:

- **Посылать отчеты по электронной почте**

  Если флажок установлен, программа отправляет сформированные отчеты по электронной почте.

  Параметры отправки отчета по электронной почте можно настроить по ссылке **Параметры отправки по электронной почте**. Ссылка доступна, когда флажок установлен.

  Если флажок снят, программа сохраняет отчеты в указанной папке для хранения отчетов.

  По умолчанию флажок снят.

- **Сохранять отчеты в папке общего доступа**

  Если флажок установлен, программа сохраняет отчеты в папке, указанной в поле под флажком. Чтобы сохранять отчеты в папке общего доступа, укажите UNC-путь к этой папке. В таком случае в окне **Выбор учетной записи для запуска задачи** необходимо задать учетную запись и пароль пользователя для доступа к этой папке.

  Если флажок снят, программа не сохраняет отчеты в папке, а отправляет их по электронной почте.

  По умолчанию флажок снят.

- **Замещать предыдущие отчеты того же типа**

  Если флажок установлен, при каждом запуске задачи новый файл отчета замещает в папке для хранения отчетов файл, сохраненный при предыдущем запуске задачи.

  Если флажок снят, файлы отчетов не перезаписываются. При каждом запуске задачи в папке сохраняется отдельный файл отчета.

  Флажок доступен, если установлен флажок **Сохранять отчет в папке**.

  По умолчанию флажок снят.

- **Задать учетную запись для доступа к папке общего доступа**

  Если флажок установлен, можно указать учетную запись, от имени которой отчет записывается в папку. Если в окне **Действия с отчетом** в качестве параметра **Сохранять отчет в папке** указан UNC-путь к папке общего доступа, необходимо указать учетную запись и пароль для доступа к этой папке.

  Если флажок снят, отчет записывается в папку от имени учетной записи Сервера администрирования.

  Флажок доступен, если установлен флажок **Сохранять отчет в папке**.

По умолчанию флажок снят.

Когда вы сохраняете или отправляете отчет в виде файла XLS, все связанные изображения, такие как логотип и датаграмма, сохраняются как отдельные файлы.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 4. Выбор учетной записи для запуска задачи

В окне **Выбор учетной записи для запуска задачи** можно указать, под какой учетной записью запускать задачу. Выберите один из следующих вариантов:

- **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.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 5. Настройка расписания задачи

В окне **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости задайте следующие параметры:

- **Запуск по расписанию:**

  Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

  - **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.

- **Каждые N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживается переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

  По умолчанию выбран этот вариант.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию 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 случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

Шаг 6. Определение названия задачи

В окне **Определение названия задачи** укажите название создаваемого правила. Название задачи не может превышать 100 символов и не может содержать специальные символы (`"*<>?\:|`).

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 7. Завершение создания задачи

В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

Работа со статистической информацией

Статистическая информация о состоянии системы защиты и управляемых устройств отображается в виде настраиваемых информационных панелей. Статистическая информация отображается в рабочей области узла **Сервер администрирования** на вкладке **Статистика**. Эта вкладка также содержит несколько вкладок второго уровня (страниц). На каждой странице отображаются информационные панели со статистической информацией, а также ссылки на корпоративные новости и другие материалы "Лаборатории Касперского". Статистическая информация представлена на информационных панелях в виде круговых или столбчатых диаграмм или таблиц. Данные на информационных панелях обновляются в процессе работы приложения и отражают текущее состояние приложения безопасности.

Можно изменить набор вкладок второго уровня, содержащихся на вкладке **Статистика**, набор информационных панелей на каждой странице с вкладками, а также способ представления данных на информационных панелях.

*Чтобы добавить новую вкладку второго уровня с информационными панелями на вкладке **Статистика**:*

1. Нажмите на кнопку **Настроить вид** в правом верхнем углу вкладки **Статистика**.

   В результате откроется окно свойств статистики. В окне содержится список страниц с вкладками, которые содержатся на вкладке **Статистика** в настоящее время. В окне можно изменять порядок отображения страниц на вкладке, добавлять и удалять страницы, переходить к настройке свойств страниц по кнопке **Свойства**.

2. Нажмите на кнопку **Добавить**.

   Откроется окно свойств новой страницы.

3. Настройте новую страницу:

   - В разделе **Общие** укажите название страницы.
   - В разделе **Информационные панели** по кнопке **Добавить** добавьте информационные панели, которые должны отображаться на странице.

     По кнопке **Свойства** в разделе **Информационные панели** можно настраивать свойства добавленных информационных панелей: название, тип и вид диаграммы в панели, данные, по которым строится диаграмма.

4. Нажмите на кнопку **ОК**.

Добавленная страница с вкладками с информационными панелями отобразится на вкладке **Статистика**. Нажав на значок параметров (⚙) можно сразу перейти к настройке страницы или выбранной информационной панели на странице.

Настройка параметров уведомлений о событиях

Kaspersky Security Center позволяет выбирать способ уведомления для администратора о событиях на клиентских устройствах и настраивать параметры уведомлений:

- Электронная почта. При возникновении события приложение посылает уведомление на указанные адреса электронной почты. Вы можете настроить текст уведомления.
- SMS. При возникновении события приложение посылает уведомления на указанные номера телефонов. Вы можете настроить отправку SMS оповещений с помощью почтового шлюза.
- Исполняемый файл. При возникновении события на устройстве, исполняемый файл запускается на рабочем месте администратора. С помощью исполняемого файла администратор может получать параметры произошедшего события.

Чтобы настроить параметры уведомлений о событиях на клиентских устройствах:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.
3. Перейдите по ссылке **Настроить параметры уведомлений и экспорта событий** и в раскрывающемся списке выберите значение **Настроить параметры уведомлений**.

   Откроется окно **Свойства: События**.

4. В разделе **Уведомление** выберите способ уведомления (электронная почта, SMS, исполняемый файл для запуска) и настройте параметры уведомлений:

   - **Электронная почта**

     На вкладке **Электронная почта** можно настроить уведомления о событиях по электронной почте.

     В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес;
- Имя устройства в сети Windows (NetBIOS-имя);
- DNS-имя SMTP-сервера.

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Если вы включите параметр **Использовать DNS и MX поиск**, вы сможете использовать несколько MX-записей IP-адреса для одного и того же DNS-имени SMTP-сервера. Одно DNS-имя может иметь несколько MX-записей с различными приоритетами полученных электронных писем. Сервер администрирования пытается отправлять уведомления по электронной почте на SMTP-сервер в порядке возрастания приоритета MX-записей. По умолчанию параметр выключен.

Если вы включили параметр **Использовать DNS и MX поиск** и не разрешили использование параметров TLS, рекомендуется использовать параметры DNSSEC на вашем серверном устройстве в качестве дополнительной меры защиты при отправке уведомлений по электронной почте.

Перейдите по ссылке **Параметры**, чтобы задать дополнительные параметры:

- Тема (название темы электронного письма).
- Адрес отправителя электронной почты.
- Параметры ESMTP-аутентификации.

Вам нужно указать учетную запись для аутентификации на SMTP-сервере, если для SMTP-сервера включен параметр ESMTP-аутентификации.

- Параметры TLS для SMTP-сервера:
  - **Не использовать TLS**

    Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

  - **Использовать TLS, если поддерживается SMTP-сервером**

    Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.

  - **Всегда использовать TLS, проверить срок действия сертификата сервера**

    Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы решите использовать значение **Всегда использовать TLS, для проверки срока действия сертификата Сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

Вы можете указать параметры TLS для SMTP-сервера:

- Выберите файл сертификата SMTP-сервера:

Вы можете получить файл со списком сертификатов от доверенного центра сертификации и загрузить его на Сервер администрирования. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также доверенным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от доверенного центра сертификации.

- Выберите файл сертификата клиента:

Вы можете использовать сертификат, полученный из любого источника, например, от любого доверенного центра сертификации. Вам нужно указать сертификат и его закрытый ключ, используя один из следующих типов сертификатов:

- Сертификат X-509:

Вам нужно указать файл с сертификатом и файл с закрытым ключом. Оба файла не зависят друг от друга. Порядок загрузки файлов не имеет значения. Когда оба файла загружены, необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

- Контейнер pkcs12:

Вам нужно загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый приложением при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив новые подстановочные параметры с подробными данными события. Список подстановочных параметров доступен по нажатию на кнопку справа от поля.

Если текст уведомления содержит знак процента (%), его нужно указать два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

Нажмите на кнопку **Отправить тестовое сообщение** можно проверить правильность настройки сообщений. Приложение отправляет тестовые сообщения на указанные адреса электронной почты.

- **SMS**

На вкладке **SMS** можно настроить отправку SMS-уведомлений о различных событиях на мобильный телефон. SMS-сообщения отправляются через почтовый шлюз.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой. Уведомления доставляются на телефоны, номера которых связаны с указанными адресами электронной почты.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес;
- Имя устройства в сети Windows (NetBIOS-имя);
- DNS-имя SMTP-сервера.

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Перейдите по ссылке **Параметры**, чтобы задать дополнительные параметры:

- Тема (название темы электронного письма).
- Адрес отправителя электронной почты.
- Параметры ESMTP-аутентификации.

Если необходимо, вы можете указать учетную запись для аутентификации на SMTP-сервере, если для SMTP-сервера включен параметр ESMTP-аутентификации.

- Параметры TLS для SMTP-сервера

Вы можете отключить использование TLS, использовать TLS, если SMTP-сервер поддерживает этот протокол, или вы можете принудительно использовать только TLS. Если вы решите использовать только TLS, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также, если вы решили использовать только TLS, вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

- Выберите файл сертификата SMTP-сервера

Вы можете получить файл со списком сертификатов от доверенного центра сертификации и загрузить его в Kaspersky Security Center. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также доверенным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от доверенного центра сертификации.

Вам нужно загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован. В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый приложением при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив новые подстановочные параметры с подробными данными события. Список подстановочных параметров доступен по нажатию на кнопку справа от поля.

Если текст уведомления содержит знак процента (%), его нужно указать два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

По кнопке **Отправить тестовое сообщение** проверьте, правильно ли настроены уведомления. Приложение отправляет тестовые сообщения указанным получателям.

- **Исполняемый файл для запуска**

Если выбран этот способ уведомления, в поле ввода можно указать, какая программа будет запущена при возникновении события.

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

По нажатию на кнопку **Отправить пробное сообщение** можно проверить правильно ли настроены сообщения: программа отправляет тестовые сообщения на указанные адреса электронной почты.

5. В поле **Текст уведомления** введите текст, который приложение будет отправлять при возникновении события.

   Из раскрывающегося списка, расположенного справа от текстового поля, можно добавлять в сообщение подстановочные параметры с деталями события (например, описание события, время возникновения и прочее).

   > Если текст уведомления содержит символ %, нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

6. По кнопке **Отправить тестовое сообщение** проверьте, правильно ли настроены уведомления.

   Приложение отправляет тестовое уведомление указанному получателю.

7. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

В результате настроенные параметры уведомления распространяются на все события, происходящие на клиентских устройствах.

Можно изменить значения параметров уведомлений для определенных событий в разделе **Настройка событий** параметров Сервера администрирования, параметров политики или параметров приложения.

Создание сертификата для SMTP-сервера

Чтобы создать сертификат для SMTP-сервера:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.
3. Перейдите по ссылке **Настроить параметры уведомлений и экспорта событий** и в раскрывающемся списке выберите значение **Настроить параметры уведомлений**.

   Откроется окно свойств событий.

4. На вкладке **Электронная почта** по ссылке **Параметры** откройте окно **Параметры**.
5. В окне **Параметры** по ссылке **Задать сертификат** откройте окно **Сертификат для подписи**.
6. В окне **Сертификат для подписи** нажмите на кнопку **Обзор**.

   Откроется окно **Сертификат**.

7. В раскрывающемся списке **Тип сертификата** выберите открытый или закрытый тип сертификата:

   - Если выбран сертификат закрытого типа (**Контейнер PKCS#12**), укажите файл сертификата и пароль.
   - Если выбран сертификат открытого типа (**X.509-сертификат**):

     a. укажите файл закрытого ключа (файл с расширением prk или pem);

     b. укажите пароль закрытого ключа;

     c. укажите файл открытого ключа (файл с расширением cer).

8. Нажмите на кнопку **OK**.

В результате будет выписан сертификат для SMTP-сервера.

Выборки событий

Информация о событиях в работе Kaspersky Security Center и управляемых приложений сохраняется как в базе данных Сервера администрирования, так и в системном журнале Microsoft Windows. Вы можете просматривать информацию из базы данных Сервера администрирования в рабочей области узла **Сервер администрирования** на вкладке **События**.

Информация на вкладке **События** представлена в виде списка выборок событий. Каждая выборка включает в себя только события определенного типа. Например, выборка "Статус устройства – Критический" содержит только записи об изменении статусов устройств на "Критический". После установки приложения на вкладке **События** содержится ряд стандартных выборок событий. Вы можете создавать дополнительные (пользовательские) выборки событий, а также экспортировать информацию о событиях в файл.

Просмотр выборки событий

Чтобы просмотреть выборку событий:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.
3. В раскрывающемся списке **Выборки событий** выберите нужную вам выборку событий.

   Если вы хотите, чтобы события этой выборки отображались в рабочей области постоянно, нажмите на значок "Избранное" (☆) рядом с выборкой.

   В результате в рабочей области будет представлен список событий выбранного типа, хранящихся на Сервере администрирования.

Вы можете сортировать информацию в списке событий по возрастанию или убыванию данных в любой графе списка.

Настройка параметров выборки событий

Чтобы настроить параметры выборки событий:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.
3. Откройте нужную вам выборку событий на вкладке **События**.
4. Нажмите на кнопку **Свойства выборки**.

В открывшемся окне свойств выборки событий вы можете настроить параметры выборки.

Создание выборки событий

Чтобы создать выборку событий:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.
3. Нажмите на кнопку **Создать выборку**.
4. В открывшемся окне **Новая выборка событий** укажите имя создаваемой выборки и нажмите на кнопку **ОК**.

В результате в раскрывающемся списке **Выборки событий** будет создана выборка с указанным вами именем.

По умолчанию созданная выборка событий содержит все события, хранящиеся на Сервере администрирования. Чтобы в выборке отображались только интересующие вас события, нужно настроить параметры выборки.

Экспорт выборки событий в текстовый файл

Чтобы экспортировать выборку событий в текстовый файл:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.
3. Нажмите на кнопку **Импорт/Экспорт**.
4. В раскрывающемся списке выберите **Экспортировать события в файл**.

В результате запустится мастер экспорта событий. Следуйте далее указаниям мастера.

Удаление событий из выборки

Чтобы удалить события из выборки:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.
3. Выберите события, которые требуется удалить, с помощью мыши и клавиш **SHIFT** или **CTRL**.
4. Удалите выбранные события одним из следующих способов:
   - В контекстном меню любого из выделенных событий выберите пункт **Удалить**.

     При выборе пункта контекстного меню **Удалить все** из выборки будут удалены все отображаемые события, независимо от того, какие из них вы предварительно выбрали для удаления.
   - По ссылке **Удалить событие**, если выбрано одно событие, или по ссылке **Удалить события**, если выбрано несколько событий, в блоке работы с выбранными событиями.

В результате выбранные события будут удалены.

Добавление приложений в исключения по запросам пользователей

Если вы получаете запросы пользователей для разблокирования ошибочно заблокированных приложений, вы можете создать исключение из правил Адаптивного контроля аномалий для этих приложений. Такие приложения больше не будут блокироваться на устройствах пользователей. Вы можете отслеживать количество запросов пользователей на вкладке **Мониторинг** в рабочей области Сервера администрирования.

Чтобы добавить приложение, заблокированное Kaspersky Endpoint Security, в исключения по запросам пользователей:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **События**.
3. В раскрывающемся списке **Выборки событий** выберите **Запросы пользователей**.
4. В контекстном меню запроса пользователя (или нескольких запросов пользователей), содержащих приложения, которые необходимо добавить в исключения, выберите пункт **Добавить исключения**.

   Запустится мастер добавления исключений. Следуйте шагам мастера.

Выбранные приложения будут исключены из списка обнаружений **Правила срабатываний в статусе Интеллектуальное обучение** (в папке **Хранилища** дерева консоли) после следующей синхронизации клиентского устройства с Сервером администрирования. Такие приложения больше не будут отображаться в списке обнаружений.

Выборки устройств

Информация о состоянии устройств содержится в дереве консоли в папке **Выборки устройств**.

Информация в папке **Выборки устройств** представлена в виде списка выборок устройств. Каждая выборка включает в себя устройства, отвечающие определенным условиям. Например, выборка **Устройства со статусом "Критический"** содержит только устройства со статусом *Критический*. После установки приложения папка **Выборки устройств** содержит ряд стандартных выборок. Вы можете создавать дополнительные (пользовательские) выборки устройств, экспортировать параметры выборок в файл, а также создавать выборки с параметрами, импортированными из файла.

Просмотр выборки устройств

Чтобы просмотреть выборку устройств:

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки в списке **Устройства выборки** выберите нужную вам выборку устройств.
3. Нажмите на кнопку **Запустить выборку**.
4. Выберите вкладку **Результаты выборки**.

В результате в рабочей области отобразится список устройств, отвечающих параметрам выборки.

Вы можете сортировать информацию в списке устройств по возрастанию или убыванию данных в любой из граф.

Настройка выборки устройств

Чтобы настроить параметры выборки устройств:

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки перейдите на вкладку **Выборка** и выберите нужную вам выборку устройств в списке пользовательских выборок устройств.
3. Нажмите на кнопку **Свойства выборки**.
4. В открывшемся окне свойств задайте следующие параметры:
   - Общие параметры выборки.
   - Условия, которые должны быть выполнены, чтобы устройство было включено в эту выборку. Чтобы настроить условия, выберите имя условия и нажмите на кнопку **Свойства**.
   - Параметры безопасности.
5. Нажмите на кнопку **OK**.

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.

Сеть

В разделе **Сеть** можно настроить критерии включения устройств в выборку на основании их сетевых данных:

- **Имя устройства или IP-адрес**

  Имя устройства в сети Windows (NetBIOS-имя) или IPv4-адрес или IPv6-адрес.

- **Windows-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.

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.

- **Тег должен присутствовать**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых есть выбранный тег. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

  По умолчанию выбран этот вариант.

- **Тег должен отсутствовать**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых нет выбранного тега. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

Active Directory

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 домена.

  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.

Сетевая активность

В разделе **Сетевая активность** можно настроить критерии включения устройств в выборку на основании их сетевой активности:

- **Это устройство 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.

Приложение

В разделе **Приложение** можно настроить критерии включения устройств в выборку на основании выбранного управляемого приложения:

- **Название приложения**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске по наименованию приложения "Лаборатории Касперского".

  В списке представлены названия только тех приложений, для которых на рабочем месте администратора установлены плагины управления.

  Если приложение не выбрано, то критерий не применяется.

- **Версия приложения**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по номеру версии приложения "Лаборатории Касперского".

  Если номер версии не указан, то критерий не применяется.

- **Название критического обновления**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по установленному для приложения наименованию или номеру пакета обновления.

  Если поле не заполнено, то критерий не применяется.

- **Последнее обновление модулей приложения**

  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 Kaspersky Security Center**

  В раскрывающемся списке можно включить в состав выборки устройства, которые находятся под управлением Kaspersky Security Center:

  - **Да**. Приложение включает в выборку устройства, которые находятся под управлением Kaspersky Security Center.
  - **Нет**. Приложение включает в выборку устройства, которые не находятся под управлением Kaspersky Security Center.
  - **Значение не выбрано**. Критерий не применяется.

- **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.

Операционная система

В разделе **Операционная система** можно настроить критерии включения устройств в выборку на основании установленной на них операционной системы.

- **Версия операционной системы**

  Если флажок установлен, в списке можно выбрать операционные системы. Устройства, на которых установлены указанные операционные системы, включаются в результаты поиска.

- **Архитектура операционной системы**

  В раскрывающемся списке можно выбрать архитектуру операционной системы, по наличию которой к устройству применяется правило перемещения (**Нет данных**, **x86**, **AMD64** или **IA64**). По умолчанию в списке не выбран ни один вариант, архитектура операционной системы не задана.

- **Версия пакета обновления операционной системы**

  В поле можно указать версию пакета установленной операционной системы (в формате *X.Y*), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

- **Номер сборки операционной системы**

  > Этот параметр применим только для операционных систем Windows.

  Номер сборки операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить поиск всех номеров сборки, кроме указанного.

- **Идентификатор выпуска операционной системы**

  > Этот параметр применим только для операционных систем Windows.

  Идентификатор выпуска операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний идентификатор выпуска. Вы также можете настроить поиск всех номеров идентификаторов выпуска, кроме указанного.

Статус устройства

В разделе **Статус устройства** можно настроить критерии включения устройств в выборку по описанию статуса устройства от управляемого приложения:

- **Статус устройства**

  Раскрывающийся список, в котором можно выбрать один из статусов устройства: *OK*, *Критический* или *Предупреждение*.

- **Описание статуса устройства**

  В этом поле можно установить флажки для условий, при соблюдении которых устройству будет присваиваться выбранный статус: *OK, Критический* или *Предупреждение*.

- **Статус устройства определен приложением**

  Раскрывающийся список, в котором можно выбрать значение статуса задачи постоянной защиты. Устройства с указанным статусом постоянной защиты будут включаться в выборку.

Компоненты защиты

В разделе **Компоненты защиты** можно настроить критерии включения устройств в выборку по состоянию защиты:

- **Дата выпуска баз**

  Если этот параметр выбран, поиск клиентских устройств выполняется по дате выпуска антивирусных баз. В полях ввода можно задать временной интервал, на основании которого будет выполняться поиск.

  По умолчанию параметр выключен.

- **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.

- **Total number of threats detected**

  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.

Реестр приложений

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.

Реестр оборудования

В разделе **Реестр оборудования** можно настроить критерии включения устройств в выборку по установленному на них оборудованию:

- **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)**

  Диапазон частот процессора. Устройства с процессорами, соответствующими диапазону частот в полях ввода (включительно), будут включены в состав выборки.

- **Виртуальных ядер процессора**

  Диапазон количества виртуальных ядер процессора. Устройства с процессорами, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем жесткого диска (ГБ)**

  Диапазон значений объема жесткого диска устройства. Устройства с жесткими дисками, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем оперативной памяти (МБ)**

  Диапазон значений объема оперативной памяти устройства. Устройства с оперативной памятью, соответствующей диапазону в полях ввода (включительно), будут включены в состав выборки.

Виртуальные машины

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:

  - **Неважно**.
  - **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:

  - **Неважно**.
  - **Нет**. Искомые устройства не должны являться частью Virtual Desktop Infrastructure.
  - **Да**. Искомые устройства должны являться частью Virtual Desktop Infrastructure (VDI).

Уязвимости и обновления

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.

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, при нажатии на кнопку **Обзор** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых последний вход в систему выполнялся указанным пользователем.

- **Пользователь, когда-либо выполнявший вход в систему**

  Если этот параметр включен, при нажатии на кнопку **Обзор** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых указанный пользователь когда-либо выполнял вход в систему.

Проблемы, связанные со статусом управляемых приложений

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.

Описание статуса устройства

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.

Статусы компонентов управляемых приложений

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, Остановлен, Запускается, Приостановлен, Выполняется, Сбой*).

- **Статус защиты для серверов совместной работы**

  Поиск устройств по статусу защиты для серверов совместной работы (*Нет данных*, *Остановлен*, *Запускается, Приостановлен*, *Выполняется*, *Сбой*).

- **Статус антивирусной защиты почтовых серверов**

  Поиск устройств по статусу защиты почтовых серверов (*Нет данных, Остановлен, Запускается, Приостановлен, Выполняется, Сбой*).

- **Статус Endpoint Sensor**

  Поиск устройств по статусу компонента Endpoint Sensor (*Нет данных, Остановлен, Запускается, Приостановлен, Выполняется, Сбой*).

Шифрование

Алгоритм шифрования

Стандарт симметричного алгоритма блочного шифрования Advanced Encryption Standard (AES). В раскрывающемся списке вы можете выбрать размер ключа шифрования (56 Бит, 128 Бит, 192 Бит или 256 Бит).

Доступные значения: *AES56*, *AES128*, *AES192*, и *AES256*.

Облачные сегменты

В разделе **Облачные сегменты** можно настроить критерии включения устройств в выборку в соответствии с облачными сегментами:

- **Устройство находится в облачном сегменте**

  Если флажок установлен, при нажатии на кнопку **Выбрать** можно указать сегмент поиска.

  Если также установлен флажок **Включая вложенные 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:

  - **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.

Компоненты приложения

> Этот раздел содержит список компонентов тех приложений, которые имеют соответствующие плагины управления, установленные в Консоли администрирования.

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*, *Остановлено*, *Запускается*, *Приостановлено*, *Выполняется*, *Сбой* или *Не установлено*. Если выбранный компонент приложения, установленный на управляемом устройстве, имеет указанный статус, устройство входит в выборку устройств.

  Статусы, отправленные приложениями:

  - *Запускается* – компонент в настоящее время находится в процессе инициализации.
  - *Выполняется* – компонент включен и работает правильно.
  - *Приостановлено* – компонент приостановлен, например, после того, как пользователь приостановил защиту в управляемом приложении.

- *Сбой* – во время выполнения операции компонента произошла ошибка.
- *Остановлено* – компонент отключен и в данный момент не работает.
- *Не установлено* – пользователь не выбрал компонент для установки во время выборочной установки приложения.

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.

Экспорт параметров выборки устройств в файл

Чтобы экспортировать параметры выборки устройств в текстовый файл:

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки на вкладке **Выборка** выберите нужную вам выборку устройств в списке пользовательских выборок устройств.

   Параметры можно экспортировать только из выборок устройств, созданных пользователем.

3. Нажмите на кнопку **Запустить выборку**.
4. На вкладке **Результаты выборки** нажмите на кнопку **Экспортировать параметры**.
5. В открывшемся окне **Сохранить как** задайте имя файла для экспорта параметров выборки, укажите папку, в которую будет сохранен файл, и нажмите на кнопку **Сохранить**.

Параметры выборки устройств будут сохранены в указанный файл.

Создание выборки устройств

Чтобы создать выборку устройств:

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите **Создать выборку**.
3. В открывшемся окне **Новая выборка устройств** укажите имя создаваемой выборки и нажмите на кнопку **OK**.

В результате в дереве консоли в папке **Выборки устройств** будет создана новая папка с указанным вами именем. По умолчанию созданная выборка устройств содержит все устройства, входящие в группы администрирования того Сервера, под управлением которого создана выборка. Чтобы в выборке отображались только интересующие вас устройства, нужно настроить параметры выборки по кнопке **Свойства выборки**.

Создание выборки устройств по импортированным параметрам

Чтобы создать выборку устройств по импортированным параметрам:

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите **Импортировать выборку из файла**.
3. В открывшемся окне укажите путь к файлу, из которого вы хотите импортировать параметры выборки. Нажмите на кнопку **Открыть**.

В результате в папке **Выборки устройств** будет создана выборка **Новая выборка**. Параметры новой выборки параметры импортированы из указанного файла.

Если в папке **Новая выборка** уже существует выборка с названием **Выборки устройств**, к имени созданной выборки добавится окончание вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

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 дереве консоли выберите папку **Выборки устройств**.
2. Выберите устройства, которые требуется удалить, с помощью клавиш **Shift** или **Ctrl**.

3. Удалите выбранные устройства из групп администрирования одним из следующих способов:

   - В контекстном меню любого из выделенных устройств выберите пункт **Удалить**.
   - Нажмите на кнопку **Выполнить действие** и в раскрывающемся списке выберите значение **Удалить из группы**.

В результате выбранные устройства будут удалены из групп администрирования, в которые они входили.

Мониторинг установки и удаления приложений

Вы можете контролировать установку и удаление определенных приложений на управляемых устройствах, например, определенного браузера. Чтобы использовать эту функцию, вы можете добавить приложения из реестра приложений в список наблюдаемых приложений. При установке или удалении контролируемого приложения Агент администрирования публикует соответствующие события: **Установлено наблюдаемое приложение** или **Удалено наблюдаемое приложение**. Вы можете контролировать эти события, используя, например, выборки событий или отчеты.

Вы можете контролировать эти события, только если они хранятся в базе данных Сервера администрирования.

Чтобы добавить приложение в список наблюдаемых приложений:

1. В дереве консоли в папке **Дополнительно** → **Управление приложениями** выберите вложенную папку **Реестр приложений**.
2. Нажмите на кнопку **Открыть окно свойств реестра приложений** над отобразившимся списком приложений.
3. В открывшемся окне **Наблюдаемые приложения** нажмите на кнопку **Добавить**.
4. В открывшемся окне **Выберите название приложения** в реестре приложений выберите, для каких приложений вы хотите контролировать установку и удаление.
5. В окне **Выберите название приложения** нажмите на кнопку **ОК**.

После того, как вы настроили список контролируемых приложений, и наблюдаемое приложение было установлено или удалено с управляемых устройств в вашей организации, вы можете контролировать соответствующие события, например, с помощью выборки событий Последние события.

События компонентов Kaspersky Security Center

Каждый компонент Kaspersky Security Center имеет собственный набор типов событий. В этом разделе перечислены типы событий, которые происходят на Сервере администрирования Kaspersky Security Center, Агенте администрирования и Сервере iOS MDM. 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, когда вы настраиваете события и при их возникновении.
- **Идентификатор типа события**. Этот цифровой код используется при обработке событий с использованием инструментов анализа событий сторонних производителей.
- **Тип события** (буквенный код). Этот код используется при просмотре и обработке событий с использованием публичных представлений базы данных Kaspersky Security Center и при экспорте событий в SIEM-системы.
- **Описание**. Этот текст содержит описание ситуации при возникновении события и описание того, что вы можете сделать в этом случае.
- **Срок хранения по умолчанию**. Это количество дней, в течение которых событие хранится в базе данных Сервера администрирования и отображается в списке событий Сервера администрирования. После окончания этого периода событие удаляется. Если значение времени хранения события указано 0, такие события регистрируются, но не отображаются в списке событий Сервера администрирования. Если вы настроили хранение таких событий в журнале событий операционной системы, вы можете найти их там.

  Можно изменить время хранения событий:

  - Консоль администрирования: Настройка срока хранения события.
  - Kaspersky Security Center Web Console: Настройка срока хранения события.

Другие данные могут включать следующие поля:

- **event_id**: уникальный номер события в базе данных, генерируемый и присваиваемый автоматически. Его не нужно путать с **Идентификатором типа события**.
- **task_id**: идентификатор задачи, в результате выполнения которой возникло событие (если такая есть).
- **severity**: один из следующих уровней важности (в порядке возрастания важности):

  0) Недопустимый уровень важности.

  1) Информационное.

  2) Предупреждение.

  3) Ошибка.

  4) Критическое.

События Сервера администрирования

В этом разделе содержится информация о событиях Сервера администрирования.

Критические события Сервера администрирования

В таблице ниже приведены типы событий Сервера администрирования Kaspersky Security Center с уровнем важности **Критическое**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Если вы указали порт в окне свойств Сервера администрирования в Консоли администрирования, **Kaspersky Security Center публикует его метрики** и критические события, которые будет получать Prometheus (система мониторинга и оповещения). Prometheus получает метрики и критические события, а затем генерирует алерты для каждого события.

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Лицензионное ограничение превышено	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Один раз в день Kaspersky Security Center проверяет, не 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 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
Файл ключа добавлен в список запрещенных	4124	KLSRV_LICENSE_BLACKLISTED	События этого типа возникают, если "Лаборатория Касперского" добавила код активации или файл ключа, который вы используете, в список запрещенных. Обратитесь в Службу технической поддержки для получения подробной информации.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Режим ограниченной функциональности	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	События этого типа возникают, если Kaspersky Security Center 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 (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. Вы не можете изменить количество дней. Если Сервер администрирования выключен, в указанный день окончания срока действия лицензии, событие не будет опубликовано до следующего дня. После окончания срока действия коммерческой лицензии, Kaspersky Security Center работает в режиме Базовой функциональности. Вы можете ответить на событие следующими способами: • Убедитесь, что резервный лицензионный ключ добавлен на Сервер администрирования. • Если вы используете подписку, продлите ее. Неограниченная подписка продлевается автоматически, если предоплата поставщику услуг была своевременно внесена.	180 дней
Срок действия сертификата истек	4132	KLSRV_CERTIFICATE_EXPIRED	События этого типа возникают, если истек срок действия клиентского сертификата на мобильных устройствах.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Срок действия сертификата Сервера администрирования истек.	6129	ServerCertificateExpired	События этого типа возникают, если истек срок действия сертификатов Сервера администрирования для мобильных устройств и для устройств с защитой на уровне UEFI в сети. Вам необходимо обновить сертификат, срок действия которого истек.	180 дней
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 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 типы событий Сервера администрирования Kaspersky Security Center с уровнем важности **Отказ функционирования**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

События отказа функционирования Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Ошибка времени выполнения	4125	KLSRV_RUNTIME_ERROR	События этого типа возникают из-за неизвестных проблем. Чаще всего это проблемы СУБД, проблемы с сетью и другие проблемы с программным и аппаратным обеспечением. Подробную информацию о событии можно найти в его описании.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Для одной из групп лицензионных приложений превышено ограничение числа установок	4126	KLSRV_INVLICPROD_EXCEDED	Сервер администрирования генерирует события такого типа периодически (каждый час). События этого типа возникают, если в Kaspersky Security Center вы управляете лицензионными ключами приложений сторонних производителей и если количество установок превысило заданное в лицензионном ключе приложения стороннего производителя ограничение. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите приложение стороннего производителя с устройств, на которых оно не используется. • Используйте лицензию стороннего производителя на большее количество устройств. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений. В группу лицензионных приложений входят приложения сторонних производителей, отвечающие заданным вами критериям.	180 дней
Не удалось выполнить 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
Не удалось выполнить копирование обновлений в заданную папку	4123	KLSRV_UPD_REPL_FAIL	События этого типа возникают, если обновления программного обеспечения копируются в общую папку (или папки). Вы можете ответить на событие следующими способами: • Проверить, имеет ли учетная запись пользователя, которая используется для получения доступа к папке (или папкам), права на запись. • Проверить, были ли изменены имя пользователя и/или пароль к папкам. • Проверить подключение к интернету, так как это может быть причиной события. Следуйте инструкциям по обновлению баз и модулей приложений.	180 дней
Нет свободного места на диске	4107	KLSRV_DISK_FULL	События этого типа возникают, если на жестком диске устройства, на котором установлен Сервер администрирования, заканчивается дисковое пространство. Освободите дисковое пространство на устройстве.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Общая папка недоступна	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	События этого типа возникают, если общая папка Сервера администрирования недоступна. Вы можете ответить на событие следующими способами: • Убедитесь, что Сервер администрирования (на котором находится общая папка) включен и доступен. • Проверьте, были ли изменены имя пользователя и/или пароль к папке. • Проверьте подключение к сети.	180 дней
База данных Сервера администрирования недоступна	4109	KLSRV_DATABASE_UNAVAILABLE	События этого типа возникают, если база Сервера администрирования становится недоступной. Вы можете ответить на событие следующими способами: • Проверьте, доступен ли удаленный сервер, на котором установлен SQL-сервер. • Просмотрите журналы событий СУБД и найдите причину недоступности базы Сервера администрирования. Например, из-за профилактических работ удаленный сервер с установленным SQL Server может быть недоступен.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Недостаточно места в базе данных Сервера администрирования	4110	KLSRV_DATABASE_FULL	События этого типа возникают, если нет свободного места в базе Сервера администрирования. Сервер администрирования не работает, если его база данных переполнена и дальнейшая запись в базу данных невозможна. Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие: • Вы используете SQL Server Express Edition: Проверьте в документации к SQL Server Express ограничение размера базы данных для используемой версии. Возможно, ваша база данных Сервера администрирования превысила ограничение размера базы данных. Ограничьте количество событий, хранящихся в базе данных Сервера администрирования. В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль приложений. Вы можете изменить параметры политики Kaspersky Endpoint Security для Windows, касающиеся хранения событий компонента Контроль приложений в базе данных Сервера администрирования. • Вы используете СУБД, отличную от SQL Server Express Edition: Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования. Сократите список событий для хранения в базе данных Сервера администрирования. Просмотрите информацию о выборе СУБД.	180 дней

События предупреждения Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Обнаружено получение частого события		KLSRV_EVENT_SPAM_EVENTS_DETECTED	События этого типа возникают, если Сервер администрирования регистрирует частые события на управляемом устройстве. Дополнительную информацию см. в следующих разделах: Блокировка частых событий.	90 дней
Лицензионное ограничение превышено	4098	KLSRV_EV_LICENSE_CHECK_100_110	Один раз в день Kaspersky Security Center 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 определяет правила генерации событий при превышении лицензионного ограничения.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Устройство долго не проявляет активности в сети	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	События этого типа возникают, если управляемое устройство неактивно в течение некоторого времени. Чаще всего это происходит, когда управляемое устройство выводится из эксплуатации. Вы можете ответить на событие следующими способами: • Удалите устройство из списка управляемых устройств вручную. • Укажите интервал, по истечении которого создается событие **Устройство долго не проявляет активности в сети** с помощью Консоли администрирования или с помощью Kaspersky Security Center Web Console. • Укажите интервал, по истечении которого устройство автоматически удаляется из группы с помощью Консоли администрирования или Kaspersky Security Center Web Console.	90 дней
Конфликт имен устройств	4102	KLSRV_EVENT_HOSTS_CONFLICT	События этого типа возникают, если Сервер администрирования рассматривает два или более управляемых устройства как одно устройство. Чаще всего это происходит, когда клонированный жесткий диск использовался для развертывания приложений на управляемых устройствах и без переключения Агента администрирования в режим клонирования выделенного диска на эталонном устройстве. Чтобы избежать этой проблемы, перед клонированием жесткого диска этого устройства переключите Агент администрирования в режим клонирования диска на эталонном устройстве.	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 превышено ограничение числа установок	4127	KLSRV_INVLICPROD_FILLED	События этого типа возникают, если количество установок приложений сторонних производителей, включенных в группу лицензионных приложений, достигает 90% от максимально допустимого значения, указанного в свойствах лицензионного ключа. Вы можете ответить на событие следующими способами: • Если приложение стороннего производителя не используется на каких-то управляемых устройствах, удалите приложение с этих устройств. • Если вы ожидаете, что количество установок для приложения стороннего производителя превысит разрешенное ограничение в ближайшем будущем, рассмотрите возможность получения лицензии приложения стороннего производителя на большее количество устройств заранее. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений.	90 дней
Сертификат запрошен	4133	KLSRV_CERTIFICATE_REQUESTED	События этого типа возникают, если не удается автоматически перевыпустить сертификат для Управления мобильными устройствами. Ниже приведены возможные причины событий и соответствующие действия по реагированию на событие: • Автоматический перевыпуск был инициирован для сертификата, для которого параметр **Автоматически перевыпускать сертификат, если это возможно**. 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 сертификата истекает.	6128	ServerCertificateExpiresSoon	События этого типа возникают, если истек срок действия сертификатов Сервера администрирования для мобильных устройств и для устройств с защитой на уровне UEFI в сети. Вам необходимо обновить сертификат, срок действия которого истек.	90 дней
Срок действия APNs-сертификата истек	4135	KLSRV_APN_CERTIFICATE_EXPIRED	События этого типа происходят, если истекает срок действия APNs-сертификата. Вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM.	Не хранится
Срок действия APNs-сертификата истекает	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	События этого типа возникают, если до истечения срока действия APNs-сертификата остается менее 14 дней. При истечении срока действия APNs-сертификата, вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM. Рекомендуется запланировать обновление APNs-сертификата до истечения срока его действия.	Не хранится

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось отправить FCM-сообщение на мобильное устройство	4138	KLSRV_GCM_DEVICE_ERROR	События этого типа возникают, если Управление мобильными устройствами настроено на использование 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 Firebase (см. главу "Downstream message error response codes").	90 дней
HTTP-ошибка при отправке FCM-сообщения на FCM-сервер	4139	KLSRV_GCM_HTTP_ERROR	События этого типа возникают, если Управление мобильными устройствами настроено на использование 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 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

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось отправить FCM-сообщение на FCM-сервер	4140	KLSRV_GCM_GENERAL_ERROR	События этого типа возникают из-за непредвиденных ошибок на стороне Сервера администрирования при работе с HTTP-протоколом Firebase Cloud Messaging. Прочтите информацию в описании события и отреагируйте соответствующим образом. Если вы не можете найти решение проблемы самостоятельно, рекомендуем вам обратиться в Службу технической поддержки "Лаборатории Касперского".	90 дней
Мало свободного места на жестком диске	4105	KLSRV_NO_SPACE_ON_VOLUMES	События этого типа возникают, если на устройстве, на котором установлен Сервер администрирования, почти закончилось дисковое пространство. Освободите дисковое пространство на устройстве.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Мало свободного места в базе Сервера администрирования	4106	KLSRV_NO_SPACE_IN_DATABASE	События этого типа возникают, если свободное место в базе Сервера администрирования ограничено. Если вы не устраните эту проблему, скоро база данных Сервера администрирования достигнет своей емкости и Сервер администрирования не будет работать. Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие. Вы используете SQL Server Express Edition: • Проверьте в документации к SQL Server Express ограничение размера базы данных для используемой версии. Возможно, ваша база данных Сервера администрирования достигла ограничения размера базы данных. • Ограничьте количество событий, хранящихся в базе данных Сервера администрирования. • В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль приложений. Вы можете изменить параметры политики Kaspersky Endpoint Security для Windows, касающиеся хранения событий компонента Контроль приложений в базе данных Сервера администрирования. Вы используете СУБД, отличную от SQL Server Express Edition: • Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования. • Сократите список событий для хранения в базе данных Сервера администрирования. Просмотрите информацию о выборе СУБД.	90 дней
Разорвано соединение с подчиненным Сервером администрирования	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	События этого типа возникают при разрыве соединения с подчиненным Сервером администрирования. Прочтите журнал событий Kaspersky Event Log на устройстве, на котором установлен подчиненный Сервер администрирования, и отреагируйте соответствующим образом.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Разорвано соединение с главным Сервером администрирования	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	События этого типа возникают при разрыве соединения с главным Сервером администрирования. Прочтите журнал событий Kaspersky Event Log на устройстве, на котором установлен главный Сервер администрирования, и отреагируйте соответствующим образом.	90 дней
Зарегистрированы новые обновления модулей 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 Консоли администрирования или 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

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Аудит (Не удалось выполнить тестовое подключение к SIEM-серверу)	5120	KLAUD_EV_SIEM_TEST_FAILED	События этого типа возникают, если не удалось подключится к SIEM-серверу.	30 дней
Не удалось выписать сертификат автоматически		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	Это событие возникает в случае ошибки создания клиентского сертификата для мобильного устройства (устройства, работающего по мобильному протоколу).	90 дней

Информационные события Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Информационное сообщение**.

Информационные события Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию	Комментарий
Лицензионный ключ использован более чем на 90%	4097	KLSRV_EV_LICENSE_CHECK_90	30 дней	
Обнаружено новое устройство	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 дней	
Устройство автоматически добавлено в группу	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 дней	
Устройство было автоматически перемещено с помощью правила	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 дней	
Устройство удалено из группы: долгое отсутствие активности в сети	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 дней	
Для одной из групп лицензионных приложений число разрешенных установок исчерпано более чем на 95%	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 дней	
Появились файлы для отправки на анализ в "Лабораторию Касперского"	4131	KLSRV_APS_FILE_APPEARED	30 дней	
Идентификатор экземпляра FCM мобильного устройства изменен	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 дней	
Обновления успешно скопированы в заданную папку	4122	KLSRV_UPD_REPL_OK	30 дней	
Установлено соединение с подчиненным Сервером администрирования	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 дней	

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию	Комментарий
Установлено соединение с главным Сервером администрирования	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 дней	
Базы обновлены	4144	KLSRV_UPD_BASES_UPDATED	30 дней	
Аудит: Подключение к Серверу администрирования	4147	KLAUD_EV_SERVERCONNECT	30 дней	
Аудит: Изменение объекта	4148	KLAUD_EV_OBJECTMODIFY	30 дней	Это событие отслеживает изменения в следующих объектах: • группах администрирования; • группах безопасности; • пользователях; • инсталляционных пакетах; • задачах; • политиках; • Серверах; • виртуальный Сервер.
Аудит: Изменение статуса объекта	4150	KLAUD_EV_TASK_STATE_CHANGED	30 дней	Например, это событие возникает, если задача завершилась ошибкой.
Аудит: Изменение параметров группы	4149	KLAUD_EV_ADMGROUP_CHANGED	30 дней	
Аудит: Подключение к Серверу администрирования было прервано	4151	KLAUD_EV_SERVERDISCONNECT	30 дней	
Аудит: Свойства объекта были изменены	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 дней	Это событие отслеживает изменения в следующих параметрах: • пользователь; • лицензия; • Сервер; • виртуальный Сервер.
Аудит: Права пользователя были изменены	4153	KLAUD_EV_OBJECTACLMODIFIED	30 дней	
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	События этого типа возникают при успешном подключении к SIEM-серверу.

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию	Комментарий
Резервный сертификат создан		ServerReserveCertificateCreated	30 дней	События этого типа возникают, если сертификат Сервера администрирования создан.
Сертификат обновлен		ServerCertificateRenewed	30 дней	События этого типа возникают, если сертификат Сервера администрирования был обновлен.
Сертификат успешно выписан автоматически		KLSRV_CERTIFICATE_AUTO_ISSUED	30 дней	Это событие происходит при успешном создании сертификата для мобильного устройства (устройства, работающего по мобильному протоколу).

События **Резервный сертификат создан**, **Сертификат обновлен** и **Сертификат успешно выписан автоматически** публикуются Сервером администрирования автоматически и отображаются в Консоли администрирования только при выполнении соответствующих этим событиям операций для сертификатов Сервера администрирования для мобильных устройств и устройств с защитой на уровне UEFI.

События Агента администрирования

В этом разделе содержится информация о событиях Агента администрирования.

События отказа функционирования Агента администрирования

В таблице ниже приведены типы событий 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 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
Управление учетными записями: ошибки	7723	KLNAG_EV_USR_MNG_ERR	Общее событие предупреждения.	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
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

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
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
Обнаружен файл sudoers, который не соответствует референсному значению	7724	KLNAG_EV_SUDOER_DIFFERENT	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	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
Новое устройство добавлено	7708	KLNAG_EV_DEVICE_ARRIVAL	30 дней
Устройство удалено	7709	KLNAG_EV_DEVICE_REMOVE	30 дней
Обнаружено новое устройство	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 дней
Устройство авторизовано	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 дней
Совместный доступ к рабочему столу Windows: файл был прочитан	7712	KLUSRLOG_EV_FILE_READ	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
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

События Сервера iOS MDM

В этом разделе содержится информация о событиях Сервера iOS MDM.

События отказа функционирования Сервера iOS MDM

В таблице ниже приведены события Сервера iOS MDM 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.

События отказа функционирования Сервера iOS MDM

Отображаемое имя типа события	Тип события	Срок хранения по умолчанию
Не удалось запросить список профилей	PROFILELIST_COMMAND_FAILED	30 дней
Не удалось установить профиль	INSTALLPROFILE_COMMAND_FAILED	30 дней
Не удалось удалить профиль	REMOVEPROFILE_COMMAND_FAILED	30 дней
Не удалось запросить список provisioning-профилей	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 дней
Не удалось установить provisioning-профиль	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 дней
Не удалось удалить provisioning-профиль	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 дней
Не удалось запросить список цифровых сертификатов	CERTIFICATELIST_COMMAND_FAILED	30 дней
Не удалось запросить список установленных приложений	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 дней
Не удалось запросить общую информацию о мобильном устройстве	DEVICEINFORMATION_COMMAND_FAILED	30 дней
Не удалось запросить информацию о безопасности	SECURITYINFO_COMMAND_FAILED	30 дней

Отображаемое имя типа события	Тип события	Срок хранения по умолчанию
Не удалось заблокировать мобильное устройство	DEVICELOCK_COMMAND_FAILED	30 дней
Не удалось очистить пароль	CLEARPASSCODE_COMMAND_FAILED	30 дней
Не удалось удалить данные мобильного устройства	ERASEDEVICE_COMMAND_FAILED	30 дней
Не удалось установить приложение	INSTALLAPPLICATION_COMMAND_FAILED	30 дней
Не удалось установить код погашения для приложения	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 дней
Не удалось запросить список управляемых приложений	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 дней
Не удалось удалить управляемое приложение	REMOVEAPPLICATION_COMMAND_FAILED	30 дней
Параметры роуминга отклонены	SETROAMINGSETTINGS_COMMAND_FAILED	30 дней
Произошла ошибка в работе приложения	PRODUCT_FAILURE	30 дней
Результат выполнения команды содержит неверные данные	MALFORMED_COMMAND	30 дней
Не удалось отправить уведомление (Push Notification)	SEND_PUSH_NOTIFICATION_FAILED	30 дней
Не удалось отправить команду	SEND_COMMAND_FAILED	30 дней
Устройство не найдено	DEVICE_NOT_FOUND	30 дней

События предупреждения Сервера iOS MDM

В таблице ниже приведены события Сервера iOS MDM 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 Сервера iOS MDM

Отображаемое имя типа события	Тип события	Срок хранения по умолчанию
Попытка подключения заблокированного мобильного устройства	INACTICE_DEVICE_TRY_CONNECTED	30 дней
Профиль удален	MDM_PROFILE_WAS_REMOVED	30 дней
Попытка повторного использования клиентского сертификата	CLIENT_CERT_ALREADY_IN_USE	30 дней
Обнаружено неактивное устройство	FOUND_INACTIVE_DEVICE	30 дней
Требуется код погашения	NEED_REDEMPTION_CODE	30 дней
Профиль, входящий в состав политики, удален с устройства	UMDM_PROFILE_WAS_REMOVED	30 дней

Информационные события Сервера iOS MDM

В таблице ниже приведены события Сервера iOS MDM 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.

Отображаемое имя типа события	Тип события	Срок хранения по умолчанию
Подключено новое мобильное устройство	NEW_DEVICE_CONNECTED	30 дней
Запрос списка профилей выполнен успешно	PROFILELIST_COMMAND_SUCCESSFULL	30 дней
Установка профиля выполнена успешно	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 дней
Удаление профиля выполнено успешно	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 дней
Запрос списка provisioning-профилей выполнен успешно	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 дней
Установка provisioning-профиля выполнена успешно	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 дней
Удаление provisioning-профиля выполнено успешно	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 дней
Запрос списка цифровых сертификатов выполнен успешно	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 дней
Запрос списка установленных приложений выполнен успешно	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 дней
Запрос общей информации о мобильном устройстве выполнен успешно	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 дней
Запрос информации о безопасности выполнен успешно	SECURITYINFO_COMMAND_SUCCESSFULL	30 дней
Мобильное устройство успешно заблокировано	DEVICELOCK_COMMAND_SUCCESSFULL	30 дней
Очистка пароля выполнена успешно	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 дней
Данные удалены с мобильного устройства	ERASEDEVICE_COMMAND_SUCCESSFULL	30 дней
Установка приложения выполнена успешно	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 дней
Установка кода погашения для приложения прошла успешно	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 дней
Запрос списка управляемых приложений выполнен успешно	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 дней
Удаление управляемого приложения выполнено успешно	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 дней
Параметры роуминга применены успешно	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 дней

Блокировка частых событий

В этом разделе представлена информация о частых событиях, блокировке отмене блокировки частых событий, экспорте списка частых событий в файл.

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.

Заблокированные события можно проверить 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 отменить блокировку и продолжать получать частые сообщения. Также можно заблокировать получение частых событий, которые вы разблокировали ранее.

Чтобы управлять блокировкой частых событий:

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Блокировка частых событий**.
3. В разделе **Блокировка частых событий**:
   - Выберите параметр **Тип события** для событий, получение которых вы хотите заблокировать.
   - Отмените выбор параметра **Тип события** для событий, которые вы хотите получать и дальше.
4. Нажмите на кнопку **Применить**.
5. Нажмите на кнопку **ОК**.

Сервер администрирования получает частые события, для которых вы отменили выбор параметра **Тип события**, и блокирует получение частых событий, для которых вы выбрали параметр **Тип события**.

Отмена блокировки частых событий

Вы можете отменить блокировку частых событий и начать получение событий до тех пор, пока Сервер администрирования снова не заблокирует этот тип частых событий.

Чтобы отменить блокировку частых событий:

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Блокировка частых событий**.
3. В разделе **Блокировка частых событий** нажмите строку частого события, для которого вы хотите отменить блокировку.
4. Нажмите на кнопку **Удалить**.

Частое событие удаляется из списка частых событий. Сервер администрирования будет получать события этого типа.

Экспорт списка частых событий в файл

Чтобы экспортировать список частых событий в файл:

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Блокировка частых событий**.
3. Нажмите на кнопку **Экспортировать в файл**.
4. В открывшемся окне **Сохранить как** укажите путь к файлу, в который вы хотите сохранить список.
5. Нажмите на кнопку **Сохранить**.

Все записи списка частых событий экспортируются в файл.

Контроль изменения состояния виртуальных машин

Сервер администрирования хранит информацию о состоянии управляемых устройств, например, реестр оборудования и список установленных приложений, параметры управляемых приложений, задач и политик. Если управляемым устройством является виртуальная машина, пользователь может в любой момент восстановить ее состояние из образа виртуальной машины (snapshot), сделанного ранее. В результате информация о состоянии виртуальной машины на Сервере администрирования может стать неактуальной.

Например, администратор создал политику защиты на Сервере администрирования в 12:00, которая начала работать на виртуальной машине VM_1 в 12:01. В 12:30 пользователь виртуальной машины VM_1 изменил ее статус, восстановив ее из снимка, сделанного в 11:00. Политика защиты перестает работать на виртуальной машине. Однако на Сервере администрирования сохранится неактуальная информация о том, что политика защиты на виртуальной машине VM_1 продолжает действовать.

Kaspersky Security Center позволяет контролировать изменение состояния виртуальных машин.

После каждой синхронизации с устройством Сервер администрирования формирует уникальный идентификатор, который хранится как на устройстве, так и на Сервере администрирования. Перед началом следующей синхронизации Сервер администрирования сравнивает значения идентификаторов на обеих сторонах. Если значения идентификаторов не совпадают, Сервер администрирования считает виртуальную машину восстановленной из образа. Сервер администрирования сбрасывает действующие для этой виртуальной машины параметры политик и задач и отправляет на нее актуальные политики и список групповых задач.

Отслеживание состояния антивирусной защиты с помощью информации в системном реестре

Чтобы отследить состояние антивирусной защиты на клиентском устройстве с помощью информации, записанной Агентом администрирования в системный реестр, в зависимости от операционной системы устройства:

- На устройствах под управлением Windows:

  1. Откройте системный реестр клиентского устройства (например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**).

  2. Перейдите в раздел:

     - для 32-разрядной системы:

       HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState

     - для 64-разрядной системы:

       HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\Stati

     В результате в системном реестре отобразится информация о состоянии антивирусной защиты клиентского устройства.

- На устройствах под управлением Linux:

  - Информация содержится в отдельных текстовых файлах, по одному для каждого типа данных, расположенных /var/opt/kaspersky/klnagent/1103/1.0.0.0/Statistics/AVState/.

- На устройствах под управление macOS:

  - Информация содержится в отдельных текстовых файлах, по одному для каждого типа данных, расположенных /Library/Application Support/Kaspersky Lab/klnagent/Data/1103/1.0.0.0/Statistics/AVState/.

Состояние антивирусной защиты соответствует значениям ключей, описанных в таблице ниже.

Ключ (тип данных)	Значение	Описание
`Protection_LastConnected (REG_SZ)`	ДД-ММ-ГГГГ ЧЧ-ММ-СС	Дата и время (в формате UTC) последнего соединения с Сервером администрирования.
`Protection_AdmServer (REG_SZ)`	IP, DNS-имя или NetBIOS-имя	Имя Сервера администрирования, который управляет устройством.
`Protection_NagentVersion (REG_SZ)`	a.b.c.d	Номер сборки Агента администрирования, установленного на устройстве.
`Protection_NagentFullVersion (REG_SZ)`	a.b.c.d (патч1; патч2; ...; патчN)	Номер версии Агента администрирования (с патчами), установленного на устройстве.
`Protection_HostId (REG_SZ)`	Идентификатор устройства;	Идентификатор устройства.
`Protection_DynamicVM (REG_DWORD)`	0 – нет 1 – да	Агент администрирования установлен в динамический режим для VDI.
`Protection_AvInstalled (REG_DWORD)`	0 – нет 1 – да	Приложение безопасности установлено на устройстве.
`Protection_AvRunning (REG_DWORD)`	0 – нет 1 – да	Постоянная защита устройства включена.
`Protection_HasRtp (REG_DWORD)`	0 – нет 1 – да	Установлен компонент постоянной защиты.
`Protection_RtpState (REG_DWORD)`	Статус постоянной защиты:	
	0	Неизвестно.
	1	Выключен
	2	Приостановлена.
	3	Запускается.
	4	Включен.
	5	Включен с высоким уровнем защиты (максимальная защита).
	6	Включен с низким уровнем защиты (максимальная скорость).
	7	Включен с параметрами по умолчанию (рекомендуемые параметры).
	8	Включен с пользовательскими параметрами.
	9	Сбой в работе.
`Protection_LastFscan (REG_SZ)`	ДД-ММ-ГГГГ ЧЧ-ММ-СС	Дата и время (в формате UTC) последней полной проверки.
`Protection_BasesDate (REG_SZ)`	ДД-ММ-ГГГГ ЧЧ-ММ-СС	Дата и время (в формате UTC) выпуска баз приложения.

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. Нажмите правой клавишей мыши на название требуемой группы администрирования.
2. В контекстном меню выберите пункт **Свойства**.

   Откроется окно свойств группы администрирования.

3. В окне **Свойства** перейдите в раздел **Устройства**.

4. При необходимости 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.

   - **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 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. Нажмите на кнопку **ОК**.

Ваши изменения сохранены и применены.

Выключение объявлений "Лаборатории Касперского"

В Kaspersky Security Center Web Console раздел объявлений "Лаборатории Касперского" (**Мониторинг и отчеты → Объявления "Лаборатории Касперского"**) предоставляет информацию о вашей версии Kaspersky Security Center и управляемых приложениях, установленных на управляемых устройствах. Если вы не хотите получать объявления "Лаборатории Касперского", вы можете отключить эту функцию.

Объявления "Лаборатории Касперского" включают в себя информацию двух типов: объявления, связанные с безопасностью, и рекламные объявления. Вы можете выключить объявления каждого типа отдельно.

Чтобы выключить объявления, связанные с безопасностью:

1. В дереве консоли выберите Сервер администрирования, для которого нужно выключить объявления, связанные с безопасностью.

2. В контекстном меню объекта выберите пункт **Свойства**.

3. В открывшемся окне свойств Сервера администрирования в разделе **Объявления "Лаборатории Касперского"** выберите вариант **Включить отображение объявлений "Лаборатории Касперского" в Kaspersky Security Center Web Console**.

4. Нажмите на кнопку **ОК**.

Объявления "Лаборатории Касперского" выключены.

Рекламные объявления по умолчанию выключены. Вы получаете рекламные сообщения только в том случае, если вы включили Kaspersky Security Network (KSN). Вы можете выключить этот тип объявлений, отключив KSN.

Настройка точек распространения и шлюзов соединений

Структура групп администрирования в Kaspersky Security Center выполняет следующие функции:

- Задание области действия политик.

  Существует альтернативный способ применения нужных наборов параметров на устройствах с помощью *профилей политик*. В этом случае область действия 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, виртуальным и подчиненным Серверам администрирования.

- Назначение точек распространения.

При построении структуры групп администрирования следует учитывать топологию сети организации для оптимального назначения точек распространения. Оптимальное распределение точек распространения позволяет уменьшить сетевой трафик внутри сети организации.

В зависимости от организационной структуры организации и топологии сетей можно выделить следующие типовые конфигурации структуры групп администрирования:

- Один офис.

- Множество небольших изолированных офисов.

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

Типовая конфигурация точек распространения: один офис

В типовой конфигурации "один офис" все устройства находятся в сети организации и "видят" друг друга. Сеть организации может состоять из нескольких выделенных частей (сетей или сегментов сети), связанных узкими каналами.

Возможны следующие способы построения структуры групп администрирования:

- Построение структуры групп администрирования с учетом топологии сети. Структура групп администрирования не обязательно должна точно отражать топологию сети. Достаточно того, чтобы выделенным частям сети соответствовали какие-либо группы администрирования. Можно использовать автоматическое назначение точек распространения, либо назначать точки распространения вручную.

- Построение структуры групп администрирования, не отражающей топологию сети. В этом случае следует отключить автоматическое назначение точек распространения и в каждой выделенной части сети назначить одно или несколько устройств точками распространения на корневую группу администрирования, например, на группу **Управляемые устройства**. Все точки распространения окажутся на одном уровне и будут иметь одинаковую область действия "все устройства сети организации". Каждый Агент администрирования будет подключаться к той точке распространения, маршрут к которой является самым коротким. Маршрут к точке распространения можно определить с помощью утилиты tracert.

Типовая конфигурация точек распространения: множество небольших удаленных офисов

Этой типовой конфигурации соответствует множество небольших удаленных офисов, возможно, связанных с главным офисом через интернет. Каждый из удаленных офисов находится за NAT, то есть подключение из одного удаленного офиса в другой невозможно – офисы изолированы друг от друга.

Конфигурацию следует обязательно отразить в структуре групп администрирования: для каждого из удаленных офисов следует создать отдельную группу администрирования (группы **Офис 1**, **Офис 2** на рисунке ниже).



Удаленные офисы отражены в структуре групп администрирования

На каждую группу администрирования, соответствующую офису, нужно назначить одну или несколько точек распространения. Точками распространения нужно назначать устройства удаленного офиса, имеющие достаточно места на диске. Устройства, размещенные, например, в группе **Офис 1**, будут обращаться к точкам распространения, назначенным на группу администрирования **Офис 1**.

Если некоторые пользователи физически перемещаются между офисами с ноутбуками, нужно в каждом удаленном офисе дополнительно к упомянутым выше точкам распространения выбрать два и или более устройств и назначить их точками распространения на группу администрирования верхнего уровня (группа **Корневая группа для офисов** на рисунке выше).

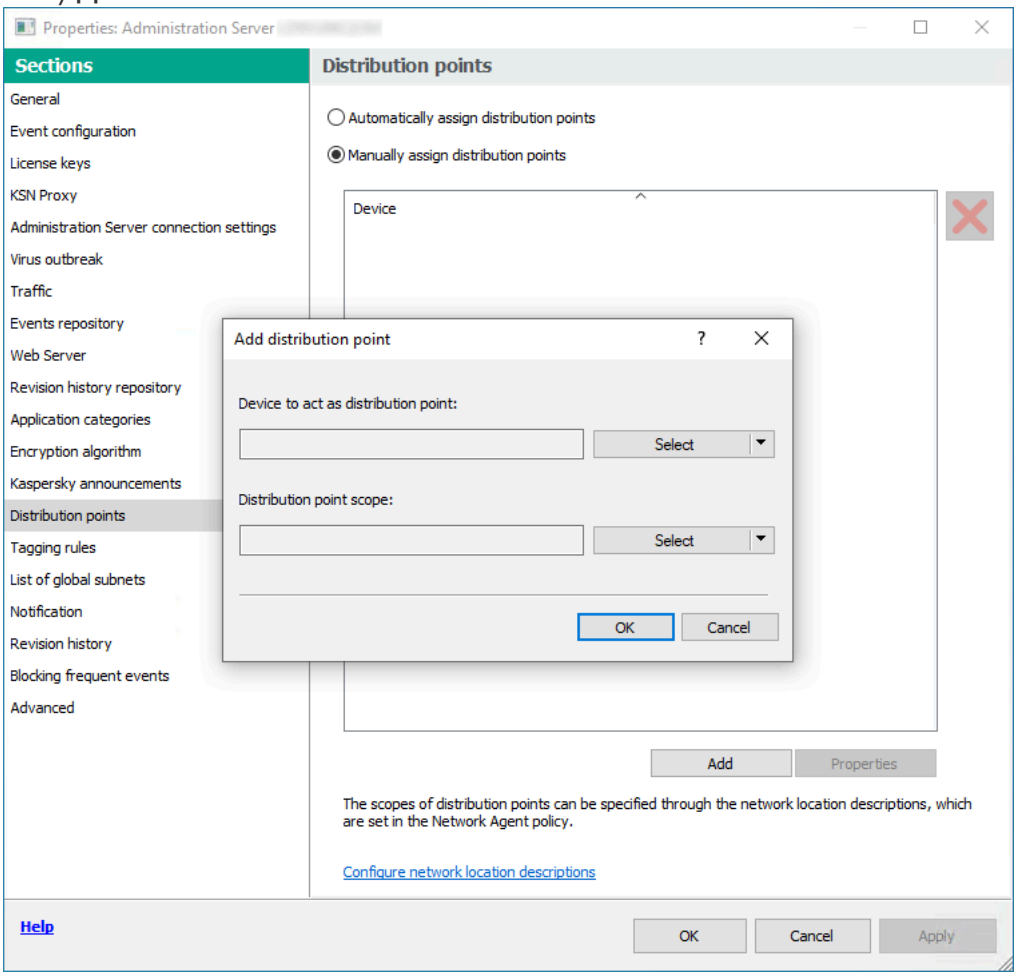
Ноутбук, находившийся в группе администрирования **Офис 1**, но физически перемещенный в офис, соответствующий группе **Офис 2**. После перемещения Агент администрирования на ноутбуке попытается обратиться к точкам распространения, назначенным на группу **Офис 1**, но эти точки распространения окажутся недоступны. Тогда Агент администрирования начнет обращаться к точкам распространения, назначенным на группу **Корневая группа для офисов**. Так как удаленные офисы изолированы друг от друга, то из всех точек распространения, назначенных на группу администрирования **Корневая группа для офисов**, успешными будут лишь обращения к точкам распространения, назначенным на группу **Офис 2**. То есть ноутбук, оставаясь в группе администрирования, соответствующей своему исходному офису, будет, тем не менее, использовать точку распространения того офиса, в котором в данный момент находится физически.

Назначение управляемого устройства точкой распространения

Вы можете вручную назначить устройство точкой распространения для группы администрирования и настроить ее как шлюз соединений в Консоли администрирования.

Чтобы назначить устройство точкой распространения группы администрирования:

1. В дереве консоли выберите узел **Сервер администрирования**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Точки распространения**.
4. В правой части окна выберите параметр **Вручную назначать точки распространения**.
5. Нажмите на кнопку **Добавить**.



Назначение точки распространения вручную

Откроется окно **Добавление точки распространения**.

6. В окне **Добавление точки распространения** выполните следующие действия:

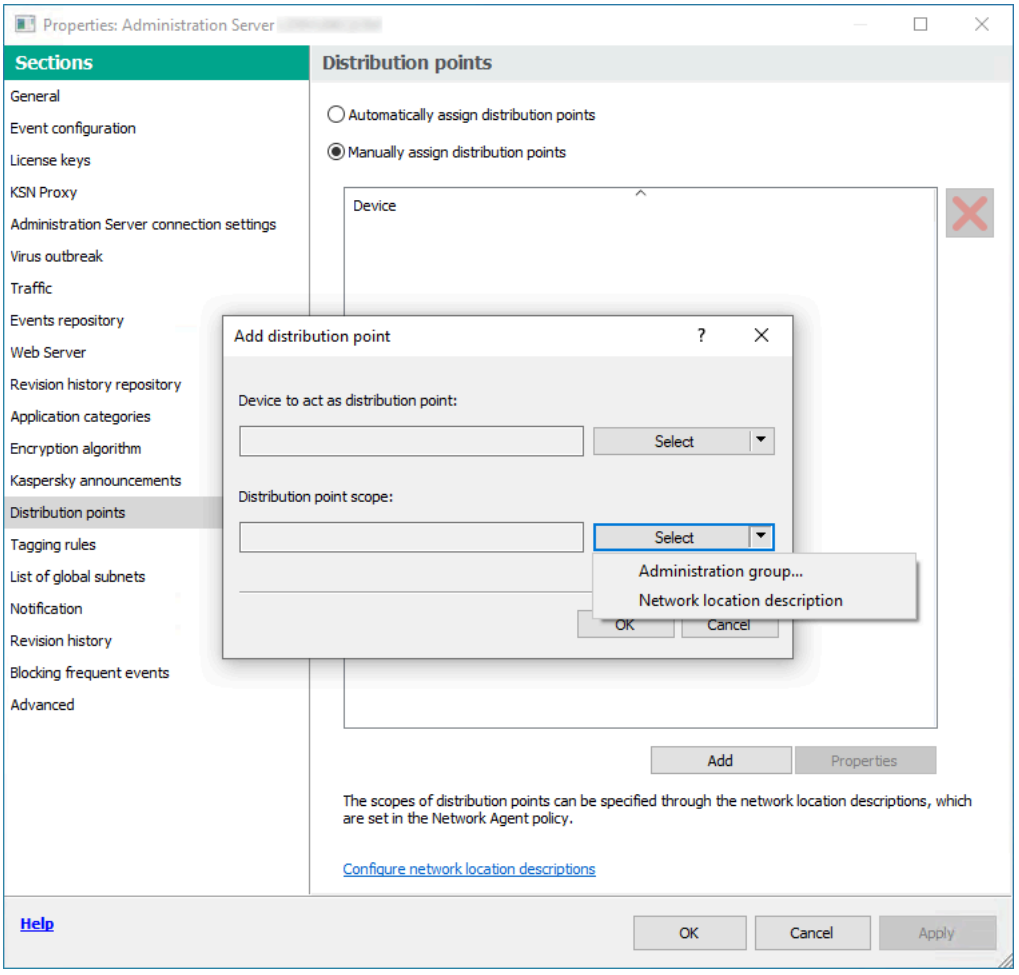
   a. В разделе **Устройство выполняет роль точки распространения** нажмите на стрелку вниз (▾) рядом с кнопкой **Выбрать** и выберите вариант **Добавить устройство из группы**.

   b. В открывшемся окне **Выбрать устройства** выберите устройство, которое будет выполнять роль точки распространения.

   c. В разделе **Область действия точки распространения** нажмите на стрелку вниз (▾) рядом с разворачивающейся кнопкой **Выбрать**.

   d. Укажите набор устройств, на которые точка распространения будет распространять обновления. Вы можете указать группу администрирования или описание сетевого местоположения.

   e. Нажмите на кнопку **OK**, чтобы закрыть окно **Добавление точки распространения**.



Выбор области действия точки распространения

Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.

Первое устройство с установленным Агентом администрирования, которое подключится к виртуальному Серверу администрирования, будет автоматически назначено точкой распространения и настроено в качестве шлюза соединений.

Подключение устройства под управлением Linux в качестве шлюза в демилитаризованной зоне

Чтобы подключить устройство под управлением Linux в качестве шлюза в демилитаризованной зоне (DMZ):

1. Загрузите и установите Агент администрирования на устройство Linux.

2. Запустите послеустановочный скрипт и следуйте указаниям мастера, чтобы настроить конфигурацию локальной среды. В командной строке выполните следующую команду:
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. На шаге с запросом режима Агента администрирования выберите параметр **Использовать как шлюз соединения**.

4. В Консоли администрирования на основе MMC в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.

5. В открывшемся окне свойств Сервера администрирования выберите раздел **Точки распространения**.

6. В открывшемся окне **Точки распространения** в правой части окна:

   a. Выберите параметр **Вручную назначать точки распространения**.

   b. Нажмите на кнопку **Добавить**.

   Откроется окно **Добавление точки распространения**.

7. В окне **Добавление точки распространения** выполните следующие действия:

   a. В разделе **Устройство выполняет роль точки распространения** нажмите на стрелку вниз (▾) рядом с разворачивающейся кнопкой **Выбрать** и выберите вариант **Добавить шлюз соединений, находящийся в демилитаризованной зоне, по адресу**.

   b. В разделе **Область действия точки распространения** нажмите на стрелку вниз (▾) рядом с разворачивающейся кнопкой **Выбрать**.

   c. Укажите набор устройств, на которые точка распространения будет распространять обновления. Вы можете указать группу администрирования.

   d. Нажмите на кнопку **ОК**, чтобы закрыть окно **Добавление точки распространения**.

8. Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.

9. Запустите утилиту klnagchk, чтобы проверить, успешно ли настроено соединение с Kaspersky Security Center. В командной строке введите команду:
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```

10. В главном меню перейдите в Kaspersky Security Center и найдите устройство.

11. В появившемся окне нажмите на <Имя устройства>.

12. В раскрывающемся списке выберите ссылку **Переместить в группу**.

13. В открывшемся окне **Выбрать группу** перейдите по ссылке **Точки распространения**.

14. Нажмите на кнопку **OK**.

15. Перезапустите службу Агента администрирования на клиенте Linux, выполнив в командной строке команду:
    ```
    $ sudo /opt/kaspersky/klnagent64/bin/klnagchk -restart
    ```

Подключение устройства под управлением Linux в качестве шлюза в демилитаризованной зоне завершено.

После этого вы можете подключить устройство под управлением Linux к Серверу администрирования с помощью настроенного шлюза соединения. Выполняйте эти процедуры только после завершения основного сценария установки.

Подключение устройства под управлением Linux к Серверу администрирования с помощью шлюза соединения

Шлюз соединения позволяет подключать клиентские устройства из демилитаризованной зоны (DMZ) к Серверу администрирования. Устройства на базе Windows и на базе Linux могут выступать в качестве шлюза соединения. После того как вы подключили и настроили шлюз соединения, вы можете использовать этот шлюз для подключения устройства под управлением Linux к Серверу администрирования. Выполняйте процедуру, описанную ниже, только после завершения основного сценария установки.

Чтобы подключить устройство под управлением Linux к Серверу администрирования с помощью шлюза соединения, выполните на этом устройстве следующие действия:

1. Загрузите и установите Агент администрирования на устройство Linux.

2. Запустите послеустановочный скрипт Агента администрирования, выполнив в командной строке следующую команду:
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. На шаге с запросом режима Агента администрирования выберите параметр **Подключаться к Серверу через шлюз соединений** и введите адрес шлюза соединения.

4. Проверьте соединение с Kaspersky Security Center и шлюзом соединения с помощью следующей команды в командной строке:
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```
   В выходных данных отображается адрес шлюза соединения.

Подключение устройства под управлением Linux к Серверу администрирования с помощью шлюза соединения завершено. Вы можете использовать это устройство для распространения обновлений, для удаленной установки приложений и для получения информации о сетевых устройствах.

Добавление шлюза соединения в демилитаризованной зоне в качестве точки распространения

Шлюз соединения ожидает соединений от Сервера администрирования, а не устанавливает соединения с Сервером администрирования. Это означает, что сразу после установки шлюза соединения на устройстве в демилитаризованной зоне Сервер администрирования не перечисляет устройство среди управляемых устройств. Следовательно, вам потребуется особая процедура, чтобы Сервер администрирования инициировал соединение со шлюзом соединения.

Чтобы добавить устройство со шлюзом соединения в качестве точки распространения:

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Точки распространения**.
4. В правой части окна выберите параметр **Вручную назначать точки распространения**.
5. Нажмите на кнопку **Добавить**.

   Откроется окно **Добавление точки распространения**.
6. В окне **Добавление точки распространения** выполните следующие действия:

   a. В разделе **Устройство выполняет роль точки распространения** нажмите на стрелку вниз (▾) рядом с разворачивающейся кнопкой **Выбрать** и выберите вариант **Добавить шлюз соединения, находящийся в демилитаризованной зоне, по адресу**.

   b. В открывшемся окне **Ввод адреса шлюза соединений** введите IP-адрес шлюза соединения (или введите имя, если шлюз соединения доступен по имени).

   c. В разделе **Область действия точки распространения** нажмите на стрелку вниз (▾) рядом с разворачивающейся кнопкой **Выбрать**.

   d. Укажите набор устройств, на которые точка распространения будет распространять обновления. Вы можете указать группу администрирования или описание сетевого местоположения.

      Рекомендуется создать отдельную группу для внешних управляемых устройств.

После того, как вы выполнили это действие, список точек распространения содержит новую запись с именем **Временная запись для шлюза соединений**.

Сервер администрирования практически сразу пытается подключиться к шлюзу соединения по указанному адресу. В случае успеха название записи меняется на имя устройства шлюза соединения. Этот процесс занимает до пяти минут.

Пока временная запись для шлюза соединения преобразуется в именованную запись, шлюз соединения также появляется в группе **Нераспределенные устройства**.

Чтобы добавить шлюз соединения в ранее настроенную сеть, переустановите Агент администрирования на устройствах, которые вы хотите подключить к вновь добавленному шлюзу соединения.

Автоматическое назначение точек распространения

Рекомендуется назначать точки распространения автоматически. Kaspersky Security Center будет сам выбирать, какие устройства назначать точками распространения.

Чтобы назначить точки распространения автоматически:

1. Откройте главное окно приложения.
2. В дереве консоли выберите узел с именем Сервера администрирования, для которого требуется автоматически назначать точки распространения.
3. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
4. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Точки распространения**.
5. В правой части окна выберите параметр **Автоматически назначать точки распространения**.

   Если автоматическое назначение устройств точками распространения включено, невозможно вручную настраивать параметры точек распространения, а также изменять список точек распространения.

6. Нажмите на кнопку **ОК**.

В результате Сервер администрирования будет автоматически назначать точки распространения и настраивать их параметры.

О локальной установке Агента администрирования на устройство, выбранное точкой распространения

Чтобы устройство, выбранное точкой распространения, могло напрямую связаться с виртуальным Сервером администрирования для выполнения роли шлюза соединений, на это устройство требуется локально установить Агент администрирования.

Порядок локальной установки Агента администрирования на устройство, выбранное точкой распространения, совпадает с порядком локальной установки Агента администрирования на любое устройство сети.

Для устройства, выбранного точкой распространения, должны быть выполнены следующие условия:

- В процессе локальной установки Агента администрирования в окне мастера установки **Сервер администрирования** в поле **Адрес Сервера** требуется указать адрес виртуального Сервера администрирования, под управлением которого находится устройство. В качестве адреса устройства можно использовать IP-адрес или имя устройства в сети Windows.

  Используется следующая форма записи адреса виртуального Сервера: <Полный адрес физического Сервера администрирования, которому подчинен виртуальный Сервер>/<Имя виртуального Сервера администрирования>.

- Для выполнения роли шлюза соединений на устройстве должны быть открыты все порты, необходимые для связи с Сервером администрирования.

В результате установки на устройство Агента администрирования с указанными параметрами приложение Kaspersky Security Center автоматически выполняет следующие действия:

- включает это устройство в группу **Управляемые устройства** виртуального Сервера администрирования;

- назначает это устройство точкой распространения группы **Управляемые устройства** виртуального Сервера администрирования.

Необходимо и достаточно выполнить локальную установку Агента администрирования на устройстве, назначенном точкой распространения группы **Управляемые устройства** в сети организации. На устройства, выполняющие роль точек распространения во вложенных группах администрирования, Агент администрирования можно установить удаленно. Для этого используйте точку распространения группы **Управляемые устройства** в качестве шлюза соединений.

Об использовании точки распространения в качестве шлюза соединений

Если Сервер администрирования находится вне демилитаризованной зоны (DMZ), Агенты администрирования, находящиеся в демилитаризованной зоне, теряют возможность соединения с ним.

Для соединения Сервера администрирования с Агентами администрирования в качестве шлюза соединений можно использовать точку распространения. Точка распространения предоставляет Серверу администрирования порт для создания соединения. В момент запуска Сервер администрирования подключается к точке распространения и не разрывает соединение с ней в течение всего времени работы.

Получив сигнал от Сервера администрирования, точка распространения посылает Агентам администрирования UDP-сигнал на подключение к Серверу администрирования. При получении сигнала Агенты администрирования подключаются к точке распространения, которая передает информацию между Агентом администрирования и Сервером администрирования. Обмен информацией может происходить по IPv4-сети или IPv6-сети.

Рекомендуется использовать в качестве шлюза соединений выделенное устройство и назначать на один шлюз соединений не более 10 000 клиентских устройств (включая мобильные устройства).

Чтобы добавить шлюз соединения в ранее настроенную сеть:

1. Установите Агент администрирования в режиме шлюза соединения.
2. Переустановите Агент администрирования на устройствах, которые вы хотите подключить к вновь добавленному шлюзу соединения.

Добавление IP-диапазонов в список диапазонов, опрашиваемых точкой распространения

Вы можете добавить IP-диапазон в список диапазонов, опрашиваемых точкой распространения.

Чтобы добавить IP-диапазон в список опрашиваемых диапазонов:

1. В дереве консоли выберите узел **Сервер администрирования**.
2. В контекстном меню узла Сервера администрирования выберите пункт **Свойства**.
3. В открывшемся окне свойств Сервера администрирования выберите раздел **Точки распространения**.
4. В списке выберите требуемую точку распространения и нажмите на кнопку **Свойства**.
5. В открывшемся окне свойств точки распространения в панели **Разделы** выберите раздел **Обнаружение устройств → IP-диапазоны**.
6. Установите флажок **Разрешить опрос диапазона**.
7. Нажмите на кнопку **Добавить**.

   Кнопка **Добавить** активна, если установлен флажок **Разрешить опрос диапазона**.

   Откроется окно **IP-диапазон**.
8. В окне **IP-диапазон** введите имя нового IP-диапазона (по умолчанию указано имя Новый диапазон).
9. Нажмите на кнопку **Добавить**.
10. Выполните одно из следующих действий:
    - Задайте IP-диапазон начальным и конечным IP-адресом.
    - Задайте IP-диапазон адресом и маской подсети.
    - Нажмите на кнопку **Обзор** и добавьте подсеть из глобального списка подсетей.
11. Нажмите на кнопку **OK**.
12. Нажмите на кнопку **OK**, чтобы добавить диапазон с заданным именем.

Новый диапазон отобразится в списке опрашиваемых диапазонов.

Использование точки распространения в качестве извещающего сервера

В Kaspersky Security Center точка распространения может работать как push-сервер для устройств, которые управляются по мобильному протоколу, и для устройств под управлением Агента администрирования. Например, push-сервер должен быть включен, если вы хотите включить принудительную синхронизацию устройств с KasperskyOS с Сервером администрирования. Push-сервер имеет ту же область управляемых устройств, что и точка распространения, на которой включен push-сервер. Если у вас есть несколько точек распространения, назначенных для одной и той же группы администрирования, вы можете включить извещающий сервер на каждой них. В этом случае Сервер администрирования распределяет нагрузку между точками распространения.

Push-сервер поддерживает нагрузку до 50 000 одновременных подключений.

Возможно, вы захотите использовать точки распространения в качестве push-серверов, чтобы обеспечить постоянную связь между управляемым устройством и Сервером администрирования. Постоянное соединение необходимо для некоторых операций, таких как запуск и остановка локальных задач, получение статистики для управляемого приложения или создание туннеля. Если вы используете точку распространения в качестве push-сервера, вам не нужно использовать параметр **Не разрывать соединение с Сервером администрирования** на управляемых устройствах или отправлять пакеты на UDP-порт Агента администрирования.

Чтобы использовать точку распространения в качестве push-сервера:

1. В дереве консоли выберите узел **Сервер администрирования**.
2. В контекстном меню узла Сервера администрирования выберите пункт **Свойства**.
3. В открывшемся окне свойств Сервера администрирования выберите раздел **Точки распространения**.
4. В списке выберите требуемую точку распространения и нажмите на кнопку **Свойства**.
5. В открывшемся окне свойств точки распространения в разделе **Общие** на левой панели **Разделы** выберите параметр **Использовать эту точку распространения как push-сервер**.
6. Укажите номер порта push-сервера, то есть того порта на точке распространения, который клиентские устройства будут использовать для подключения.

   По умолчанию номер порта – 13295.
7. Нажмите на кнопку **OK**, чтобы закрыть окно свойств точки распространения.
8. Откройте окно свойств политики Агента администрирования.
9. В разделе **Подключения** перейдите в подраздел **Сеть**.

10. В подразделе **Сеть** выберите вариант **Использовать точку распространения для принудительного подключения к Серверу администрирования**.

11. Нажмите на кнопку **OK**, чтобы закрыть окно.

    Точка распространения начинает выполнять роль push-сервера. Теперь он может отправлять push-уведомления на клиентские устройства.

Если вы управляете устройствами с установленной операционной системой KasperskyOS или планируете это сделать, вам нужно использовать точку распространения в качестве push-сервера. Вы также можете использовать точку распространения в качестве push-сервера, если хотите отправлять push-уведомления на клиентские устройства.

Другие повседневные задачи

Этот раздел содержит рекомендации о ежедневной работе с Kaspersky Security Center.

Управление Серверами администрирования

Этот раздел содержит информацию о работе с Серверами администрирования и о настройке параметров Сервера администрирования.

Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования

Вы можете добавить Сервер администрирования в качестве подчиненного Сервера, установив таким образом отношение иерархии "главный Сервер – подчиненный Сервер". Добавление возможно независимо от того, доступен ли Сервер, который вы хотите сделать подчиненным, для подключения через Консоль администрирования.

При объединении Серверов в иерархию необходимо, чтобы порт 13291 обоих Серверов был доступен. Порт 13291 необходим для приема подключений от Консоли администрирования к Серверу администрирования.

Подключение Сервера администрирования в качестве подчиненного к главному Серверу

Вы можете добавить Сервер администрирования в качестве подчиненного Сервера с подключением к главному Серверу по порту 13000. Вам потребуется устройство с установленной Консолью администрирования, с которого доступны порты TCP 13291 обоих Серверов администрирования:

Чтобы добавить Сервер администрирования, доступный для подключения через Консоль, в качестве подчиненного Сервера:

1. Убедитесь, что порт 13000 поддерживаемого главного Сервера доступен для приема подключений от подчиненных Серверов администрирования.

2. С помощью Консоли администрирования подключитесь к будущему главному Серверу администрирования.

3. Выберите группу администрирования, в которую вы планируете добавить подчиненный Сервер администрирования.

4. В рабочей области узла **Серверы администрирования** выбранной группы перейдите по ссылке **Добавить подчиненный Сервер администрирования**.

   Запустится мастер добавления подчиненного Сервера администрирования.

5. На первом шаге мастера (ввод адреса Сервера администрирования, добавляемого в группу) введите сетевое имя будущего подчиненного Сервера администрирования.

6. Следуйте далее указаниям мастера.

Отношение "Главный Сервер – подчиненный Сервер" будет установлено. Подчиненный Сервер будет принимать подключение от главного Сервера.

Если у вас нет устройства с установленной Консолью администрирования, с которого доступны порты TCP 13291 обоих Серверов администрирования (например, если будущий подчиненный Сервер находится в удаленном офисе, а системный администратор удаленного офиса из соображений безопасности не делает доступным порт 13291 через интернет), вы все равно можете добавить подчиненный Сервер.

Чтобы добавить Сервер администрирования, недоступный для подключения через Консоль, в качестве подчиненного Сервера:

1. Убедитесь, что порт 13000 будущего главного Сервера доступен для подключения от подчиненных Серверов администрирования.

2. Запишите файл сертификата будущего главного Сервера администрирования на внешнее устройство (например, съемный диск) либо перешлите системному администратору того удаленного офиса, в котором находится Сервер администрирования.

   Файл сертификата Сервера администрирования находится на Сервере администрирования по адресу %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

3. Запишите файл сертификата будущего подчиненного Сервера администрирования на внешнее устройство (например, съемный диск). Если будущий подчиненный Сервер находится в удаленном офисе, попросите системного администратора удаленного офиса переслать вам сертификат.

   Файл сертификата Сервера администрирования находится на Сервере администрирования по адресу %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

4. С помощью Консоли администрирования подключитесь к будущему главному Серверу администрирования.

5. Выберите группу администрирования, в которую вы планируете добавить подчиненный Сервер администрирования.

6. Нажмите на кнопку **Добавить подчиненный Сервер администрирования** в рабочей области узла **Серверы администрирования**.

   Запустится мастер добавления подчиненного Сервера администрирования.

7. На первом шаге мастера (ввод адреса) оставьте поле **Адрес подчиненного Сервера администрирования (необязательно)** пустым.

8. В окне **Файл сертификата подчиненного Сервера администрирования** нажмите на кнопку **Обзор** и выберите сохраненный ранее файл сертификата подчиненного Сервера.

9. После завершения работы мастера подключитесь с помощью другой Консоли администрирования к будущему подчиненному Серверу администрирования. Если этот Сервер находится в удаленном офисе, попросите системного администратора удаленного офиса подключиться к будущему подчиненному Серверу администрирования и выполнить на нем дальнейшие шаги.

10. В контекстном меню узла **Сервер администрирования** выберите **Свойства**.

11. В свойствах Сервера администрирования перейдите в раздел **Дополнительно** и затем в раздел **Иерархия Серверов администрирования**.

12. Установите флажок **Данный Сервер администрирования является подчиненным в иерархии**.

    Поля ввода станут доступными для ввода и редактирования.

13. В поле **Адрес главного Сервера администрирования** введите сетевое имя будущего главного Сервера администрирования.

14. Выберите ранее сохраненный файл сертификата будущего главного Сервера, нажав на кнопку **Обзор**.

15. Нажмите на кнопку **OK**.

Отношение "Главный Сервер – подчиненный Сервер" будет установлено. Вы сможете подключаться к подчиненному Серверу через Консоль администрирования. Подчиненный Сервер будет принимать подключение от главного Сервера.

Подключение главного Сервера администрирования к подчиненному Серверу

Вы можете добавить новый Сервер администрирования в качестве подчиненного Сервера так, чтобы главный Сервер подключался к подчиненному Серверу по порту 13000. Это целесообразно, например, если вы размещаете подчиненный Сервер в демилитаризованной зоне.

Вам потребуется устройство с установленной Консолью администрирования, с которого доступны порты TCP 13291 обоих Серверов администрирования:

Чтобы добавить новый Сервер администрирования в качестве подчиненного и подключить главный Сервер к нему по порту 13000:

1. Убедитесь, что порт 13000 будущего подчиненного Сервера доступен для приема подключений от главного Сервера администрирования.

2. С помощью Консоли администрирования подключитесь к будущему главному Серверу администрирования.

3. Выберите группу администрирования, в которую вы планируете добавить подчиненный Сервер администрирования.

4. В рабочей области узла **Серверы администрирования** нужной группы администрирования перейдите по ссылке **Добавить подчиненный Сервер администрирования**.

   Запустится мастер добавления подчиненного Сервера администрирования.

5. На первом шаге мастера (ввод адреса Сервера администрирования, добавляемого в группу) введите сетевое имя будущего подчиненного Сервера администрирования, и установите флажок **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.

6. Если вы подключаетесь к будущему подчиненному Серверу через прокси-сервер, на первом шаге мастера установите флажок **Использовать прокси-сервер** и введите параметры подключения.

7. Следуйте далее указаниям мастера.

Будет установлена иерархия Серверов администрирования. Подчиненный Сервер будет принимать подключение от главного Сервера.

Подключение к Серверу администрирования и переключение между Серверами администрирования

При запуске приложение Kaspersky Security Center предпринимает попытку соединения с Сервером администрирования. Если в сети существует несколько Серверов администрирования, запрашивается тот Сервер, с которым было установлено соединение во время предыдущего сеанса работы приложения Kaspersky Security Center.

> Если приложение запускается в первый раз после установки, выполняется попытка соединения с Сервером администрирования, указанным при установке Kaspersky Security Center.

После соединения с Сервером администрирования структура папок этого Сервера отображается в дереве консоли.

Если в дерево консоли добавлено несколько Серверов администрирования, вы можете переключаться между ними.

Для работы с каждым Сервером администрирования необходима Консоль администрирования. Перед первым подключением к новому Серверу администрирования убедитесь, что на нем открыт порт 13291, по которому принимаются подключения от Консоли, и все остальные порты для связи Сервера администрирования с другими компонентами Kaspersky Security Center.

Чтобы переключиться на другой Сервер администрирования:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.

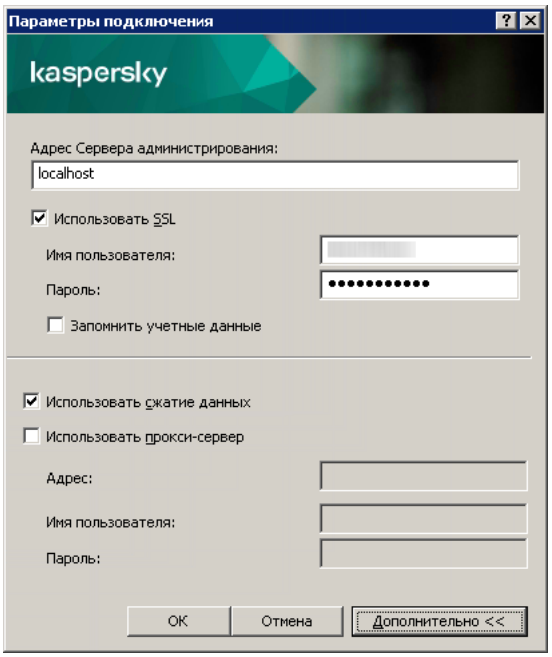
2. В контекстном меню узла Сервера администрирования выберите пункт **Подключиться к Серверу администрирования**.

3. В открывшемся окне **Параметры подключения** в поле **Адрес Сервера администрирования** укажите имя Сервера администрирования, к которому вы хотите подключиться. В качестве имени Сервера администрирования вы можете указать IP-адрес или имя устройства в сети Windows. При нажатии на кнопку **Дополнительно** в нижней части окна вы можете настроить параметры подключения к Серверу администрирования (см. рис. ниже).

Для подключения к Серверу администрирования через порт, отличный от установленного по умолчанию, в поле **Адрес Сервера администрирования** требуется ввести значение в формате <Имя Сервера администрирования>:<Порт>.

Чтобы подключиться к виртуальному Серверу администрирования, введите значение в поле **Адрес Сервера администрирования** в формате <Адрес Сервера администрирования>/<имя виртуального Сервера>.

Пользователям, не обладающим правами на **Чтение**, будет отказано в доступе к Серверу администрирования.



Процесс подключения к Серверу администрирования

4. Нажмите на кнопку **OK** для завершения переключения между Серверами.

После соединения с Сервером администрирования структура папок соответствующего ему узла в дереве консоли обновляется.

Права доступа к Серверу администрирования и его объектам

При установке Kaspersky Security Center автоматически формируются группы пользователей **KLAdmins** и **KLOperators**. Этим группам предоставляются права на подключение к Серверу администрирования и на работу с его объектами.

В зависимости от того, под какой учетной записью проводится установка Kaspersky Security Center, группы **KLAdmins** и **KLOperators** создаются следующим образом:

- Если установка проводится под учетной записью пользователя, входящего в домен, группы создаются в домене, в который входит Сервер администрирования, и на Сервере администрирования.
- Если установка проводится под учетной записью системы, группы создаются только на Сервере администрирования.

Просмотр групп **KLAdmins** и **KLOperators** и внесение необходимых изменений в права пользователей групп **KLAdmins** и **KLOperators** можно осуществлять при помощи стандартных средств администрирования операционной системы.

Группе **KLAdmins** предоставлены все права, группе **KLOperators** – права на чтение и выполнение. Набор прав, предоставленных группе **KLAdmins**, недоступен для изменения.

Пользователи, входящие в группу **KLAdmins**, называются *администраторами Kaspersky Security Center*, пользователи из группы **KLOperators** – *операторами Kaspersky Security Center*.

Помимо пользователей, входящих в группу **KLAdmins**, права администратора Kaspersky Security Center предоставляются локальным администраторам устройств, на которых установлен Сервер администрирования.

Локальных администраторов можно исключать из списка пользователей, имеющих права администратора Kaspersky Security Center.

Все операции, запущенные администраторами Kaspersky Security Center, выполняются с правами учетной записи Сервера администрирования.

Для каждого Сервера администрирования в сети можно сформировать свою группу **KLAdmins**, обладающую правами только в рамках работы с этим Сервером.

Если устройства, относящиеся к одному домену, входят в группы администрирования разных Серверов, то администратор домена является администратором Kaspersky Security Center в рамках всех этих групп администрирования. Группа **KLAdmins** для этих групп администрирования едина и создается при установке первого Сервера администрирования. Операции, запущенные администратором Kaspersky Security Center, выполняются с правами учетной записи того Сервера администрирования, для которого они запущены.

После установки приложения администратор Kaspersky Security Center может выполнять следующие действия:

- изменять права, предоставляемые группам **KLOperators**;
- определять права доступа к функциям приложения Kaspersky Security Center другим группам безопасности и отдельным пользователям, зарегистрированным на рабочем месте администратора;
- определять права доступа пользователей к работе в каждой группе администрирования.

Администратор Kaspersky Security Center может назначать права доступа к каждой группе администрирования или к другим объектам Сервера администрирования в разделе **Безопасность** окна свойств выбранного объекта.

Вы можете отследить действия пользователя при помощи записей о событиях в работе Сервера администрирования. Записи о событиях отображаются в узле **Сервер администрирования** на вкладке **События**. Эти события имеют уровень важности **Информационные события**; типы событий начинаются со слова **Аудит**.

Условия подключения к Серверу администрирования через интернет

Если Сервер администрирования является удаленным, то есть находится вне сети организации, клиентские устройства подключаются к нему через интернет.

Для подключения устройств к Серверу администрирования через интернет должны быть выполнены следующие условия:

- Удаленный Сервер администрирования должен иметь внешний IP-адрес, и на нем должен быть открыт входящий порт 13000 (для подключения от Агентов администрирования). Рекомендуется также открыть порт UDP 13000 (для приема уведомлений о выключении устройств).

- На устройствах должны быть установлены Агенты администрирования.

- При установке Агента администрирования на устройства должен быть указан внешний IP-адрес удаленного Сервера администрирования. Если для установки используется инсталляционный пакет, внешний IP-адрес требуется указать вручную в свойствах инсталляционного пакета в разделе **Параметры**.

- Для управления приложениями и задачами устройства с помощью удаленного Сервера администрирования требуется установить флажок **Не разрывать соединение с Сервером администрирования** в окне свойств этого устройства в разделе **Общие**. После установки флажка необходимо дождаться синхронизации Сервера администрирования с удаленным устройством. Непрерывное соединение с Сервером администрирования могут поддерживать не более 300 клиентских устройств одновременно.

Для ускорения выполнения задач, поступающих от удаленного Сервера администрирования, можно открыть на устройстве порт 15000. В этом случае для запуска задачи Сервер администрирования посылает специальный пакет Агенту администрирования по порту 15000, не дожидаясь синхронизации с устройством.

Защищенное подключение к Серверу администрирования

Обмен информацией между клиентскими устройствами и Сервером администрирования, а также подключение Консоли администрирования к Серверу администрирования могут производиться с использованием протокола TLS (Transport Layer Security). Протокол TLS позволяет идентифицировать стороны, взаимодействующие при подключении, осуществлять шифрование передаваемых данных и обеспечивать их защиту от изменения при передаче. В основе протокола TLS лежит аутентификация взаимодействующих сторон и шифрование данных по методу открытых ключей.

Аутентификация Сервера при подключении устройства

При первом подключении клиентского устройства к Серверу администрирования Агент администрирования на устройстве получает копию сертификата Сервера администрирования и сохраняет его локально.

> При локальной установке Агента администрирования на устройство сертификат Сервера администрирования можно выбрать вручную.

На основании полученной копии сертификата осуществляется проверка прав и полномочий Сервера администрирования при следующих соединениях.

В дальнейшем, при каждом подключении устройства к Серверу администрирования Агент администрирования запрашивает сертификат Сервера администрирования и сравнивает его с локальной копией. Если они не совпадают, доступ Сервера администрирования к устройству не разрешается.

Аутентификация Сервера при подключении Консоли администрирования

При первом подключении к Серверу администрирования Консоль администрирования запрашивает сертификат Сервера администрирования и сохраняет его копию локально на рабочем месте администратора. На основании полученной копии сертификата при последующих подключениях Консоли администрирования к этому Серверу администрирования осуществляется идентификация Сервера администрирования.

Если сертификат Сервера администрирования не совпадает с копией сертификата, хранящейся на рабочем месте администратора, Консоль администрирования выводит запрос на подтверждение подключения к Серверу администрирования с заданным именем и на получение нового сертификата. После подключения Консоль администрирования сохраняет копию нового сертификата Сервера администрирования, которая будет использоваться для идентификации Сервера в дальнейшем.

Настройка списка разрешенных IP-адресов для подключения к Серверу администрирования

По умолчанию пользователи могут войти в Kaspersky Security Center с любого устройства, на котором они могут открыть Kaspersky Security Center Web Console или на котором установлена Консоль администрирования на основе консоли Microsoft Management Console (MMC). Настроить Сервер администрирования можно таким образом, чтобы пользователи могли подключаться к нему только с устройств с разрешенными IP-адресами. В этом случае, даже если злоумышленник похитит учетную запись Kaspersky Security Center, он не сможет войти в Kaspersky Security Center, так как IP-адрес устройства злоумышленника отсутствует в списке разрешенных.

IP-адрес проверяется, когда пользователь входит в Kaspersky Security Center или запускает приложение, которое взаимодействует с Сервером администрирования через Kaspersky Security Center OpenAPI. В этот момент устройство пользователя пытается установить соединение с Сервером администрирования. Если IP-адрес устройства отсутствует в списке разрешенных, возникает ошибка аутентификации и событие KLAUD_EV_SERVERCONNECT уведомляет о том, что соединение с Сервером администрирования не установлено.

Требования к списку разрешенных IP-адресов

IP-адреса проверяются только при попытке подключения к Серверу администрирования следующих приложений:

- Сервер Kaspersky Security Center Web Console.

  Если вы входите в Web Console на одном устройстве, а Сервер Web Console установлен на другом устройстве, вы можете настроить сетевой экран на устройстве с Сервером Web Console штатными средствами операционной системы. Тогда, если кто-то попытается войти в Web Console, сетевой экран поможет предотвратить вмешательство злоумышленников.

- Консоль администрирования.

- Приложения, взаимодействующие с Сервером администрирования через объекты автоматизации klakaut.

- Приложения, взаимодействующие с Сервером администрирования через OpenAPI, такие как Kaspersky Anti Targeted Attack Platform или Kaspersky Security для виртуальных сред.

Поэтому укажите адреса устройств, на которых установлены перечисленные выше приложения.

Вы можете установить IPv4-адреса и IPv6-адреса. Указать диапазоны IP-адресов невозможно.

Как создать список разрешенных IP-адресов

Если вы еще не установили список разрешенных, следуйте приведенным ниже инструкциям.

Чтобы создать список разрешенных IP-адресов для входа в Kaspersky Security Center:

1. На устройстве Сервера администрирования запустите командную строку под учетной записью с правами администратора.
2. Измените текущую директорию на папку установки Kaspersky Security Center (обычно это <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).
3. Введите следующую команду, используя права администратора:
   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP addresses>" -t s
   ```
   Укажите IP-адреса, соответствующие перечисленным выше требованиям. Несколько IP-адресов должны быть разделены точкой с запятой.

   Пример того, как разрешить подключение к Серверу администрирования только одному устройству:

   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s
   ```

   Пример того, как разрешить нескольким устройствам подключаться к Серверу администрирования:

   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s
   ```
4. Перезапустите службу Сервера администрирования.

Узнать, успешно настроен список разрешенных IP-адресов, можно в журнале событий Kaspersky Event Log на Сервере администрирования.

Как изменить список разрешенных IP-адресов

Вы можете изменить список разрешенных точно так же, как и при его создании. Для этого выполните ту же команду и укажите новый список разрешенных:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP addresses>" -t s
```

Если вы хотите удалить некоторые IP-адреса из списка разрешенных, перепишите его. Например, ваш список разрешенных включает следующие IP-адреса: 192.0.2.0; 198.51.100.0; 203.0.113.0. Вы хотите удалить IP-адрес 198.51.100.0. Для этого в командной строке введите следующую команду:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

Не забудьте перезапустить службу Сервера администрирования.

Как сбросить настроенный список разрешенных IP-адресов

Чтобы сбросить уже настроенный список разрешенных IP-адресов:

1. Введите следующую команду в командной строке с правами администратора:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`

2. Перезапустите службу Сервера администрирования.

После этого IP-адреса больше не проверяются.

Использование утилиты klscflag для закрытия порта 13291

Порт 13291 Сервера администрирования используется для приема подключений от Консолей администрирования. По умолчанию порт открыт. Если вы не хотите использовать Консоль администрирования на основе консоли Microsoft Management Console (MMC) или утилиту klakaut, вы можете закрыть этот порт с помощью утилиты klscflag. Эта утилита изменяет значение параметра KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

Чтобы закрыть порт 13291:

1. Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Выполните следующую команду в командной строке:
   `klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`

3. Перезапустите службу Сервера администрирования Kaspersky Security Center.

   Порт 13291 закрыт.

Чтобы проверить, был ли успешно закрыт порт 13291:

Выполните следующую команду в командной строке:

```
klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

Эта команда возвращает следующий результат:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)false
```

Значение `false` означает, что порт закрыт. В противном случае отображается значение `true`.

Отключение от Сервера администрирования

Чтобы отключиться от Сервера администрирования:

1. В дереве консоли выберите узел, соответствующий Серверу администрирования, от которого нужно отключиться.

2. В контекстном меню узла выберите пункт **Отключиться от Сервера администрирования**.

Добавление Сервера администрирования в дерево консоли

Чтобы добавить в дерево консоли Сервер администрирования:

1. В главном окне приложения Kaspersky Security Center выберите в дереве консоли узел **Kaspersky Security Center**.

2. В контекстном меню узла выберите пункт **Новый → Сервер администрирования**.

В результате в дереве консоли будет создан узел с именем **Сервер администрирования – <Имя устройства> (Не подключен)**, с которого вы можете подключиться к любому из установленных в сети Серверов администрирования.

Удаление Сервера администрирования из дерева консоли

Чтобы удалить Сервер администрирования из дерева консоли:

1. В дереве консоли выберите узел, соответствующий удаляемому Серверу администрирования.

2. В контекстном меню узла выберите пункт **Удалить**.

Добавление виртуального Сервера администрирования в дерево консоли

Чтобы добавить в дерево консоли виртуальный Сервер администрирования:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования, для которого нужно создать виртуальный Сервер администрирования.

2. В узле Сервера администрирования выберите папку **Серверы администрирования**.

3. В рабочей области папки **Серверы администрирования** перейдите по ссылке **Добавить виртуальный Сервер администрирования**.

   Запустится мастер создания виртуального Сервера администрирования.

4. В окне **Имя виртуального Сервера администрирования** укажите имя создаваемого виртуального Сервера.

   Имя виртуального Сервера администрирования не может превышать 255 символов и содержать специальные символы ("*<>?\:|).

5. В окне **Ввод адреса подключения устройств к виртуальному Серверу** укажите адрес подключения устройств.

   Адрес подключения виртуального Сервера администрирования – это сетевой адрес, по которому к нему будут подключаться устройства. Адрес подключения состоит из двух частей: сетевого адреса физического Сервера администрирования и имени виртуального Сервера, разделенных символом косой черты (слешем). Имя виртуального Сервера будет подставлено автоматически. Указанный адрес будет использоваться на этом виртуальном Сервере как адрес по умолчанию в инсталляционных пакетах Агента администрирования.

6. В окне **Создание учетной записи администратора виртуального Сервера** назначьте администратором виртуального Сервера пользователя из списка или добавьте новую учетную запись для администратора по кнопке **Создать**.

   Вы можете указать несколько учетных записей.

В результате в дереве консоли будет создан узел с именем **Сервер администрирования – <Имя виртуального Сервера>**.

Смена учетной записи службы Сервера администрирования. Утилита klsrvswch

Если вам требуется изменить учетную запись службы Сервера администрирования, заданную при установке приложения Kaspersky Security Center, вы можете воспользоваться утилитой смены учетной записи Сервера администрирования klsrvswch.

При установке Kaspersky Security Center утилита автоматически копируется в папку установки приложения.

Количество запусков утилиты не ограничено.

Вам нужно запустить утилиту klsrvswch на устройстве Сервера администрирования под учетной записью с правами администратора, которая использовалась для установки Сервера администрирования.

Утилита klsrvswch позволяет менять тип учетной записи. Например, если вы используете локальную учетную запись, вы можете сменить ее на доменную учетную запись либо на управляемую учетную запись службы (и наоборот). Утилита klsrvswch не позволяет изменить тип учетной записи на групповую управляемую учетную запись службы (gMSA).

Windows Vista и более поздние версии Windows не позволяют использовать учетную запись LocalSystem для Сервера администрирования. В этих версиях операционных систем Windows учетная запись **LocalSystem** неактивна.

Чтобы изменить учетную запись службы Сервера администрирования на доменную учетную запись:

1. Запустите утилиту klsrvswch из папки установки Kaspersky Security Center. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   В результате запускается мастер изменения учетной записи службы Сервера администрирования. Следуйте далее указаниям мастера.

2. В окне **Учетная запись службы Сервера администрирования** выберите **Учетная запись LocalSystem**.

В результате работы мастера учетная запись Сервера администрирования изменяется. Служба Сервера администрирования запустится под учетной записью *LocalSystem* и будет использовать ее учетные данные.

Для правильной работы Kaspersky Security Center требуется, чтобы учетная запись для запуска службы Сервера администрирования обладала правами администратора ресурса для размещения информационной базы Сервера администрирования.

Чтобы изменить учетную запись службы Сервера администрирования на учетную запись пользователя или на управляемую учетную запись службы:

1. Запустите утилиту klsrvswch из папки установки Kaspersky Security Center. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   В результате запускается мастер изменения учетной записи службы Сервера администрирования. Следуйте далее указаниям мастера.

2. В окне **Учетная запись службы Сервера администрирования** выберите **Учетная запись пользователя**.

3. Нажмите на кнопку **Найти**.

   Откроется окно **Выбор пользователя**.

4. В окне **Выбор пользователя** нажмите на кнопку **Типы объекта**.

5. В списке типов объекта выберите **Пользователи** (если вы хотите использовать учетную запись пользователя) или **Учетная запись для служб** (если вы хотите использовать управляемую учетную запись службы) и нажмите на кнопку **ОК**.

6. В поле для имени объекта введите имя учетной записи или часть имени и нажмите на кнопку **Проверить имена**.

7. В списке соответствующих имен выберите необходимое имя и нажмите на кнопку **OK**.

8. Если вы выбрали **Учетные записи служб**, в окне **Пароль учетной записи**, оставьте поля **Пароль** и **Подтверждение пароля** пустыми. Если вы выбрали **Пользователи**, введите пароль для пользователя и подтвердите его.

Учетная запись службы Сервера администрирования будет запускаться под выбранной вами учетной записью.

При использовании Microsoft SQL-сервера в режиме аутентификации учетной записи пользователя средствами Windows требуется обеспечить доступ к базе данных. Учетная запись пользователя должна быть владельцем базы данных Kaspersky Security Center. По умолчанию требуется использовать схему dbo.

Изменение учетных данных СУБД

Вам может потребоваться изменить учетные данные СУБД, например, чтобы выполнить ротацию учетных данных в целях безопасности.

Чтобы изменить учетные данные СУБД в среде Windows с помощью утилиты klsrvswch.exe:

1. Запустите утилиту klsrvswch, которая расположена в папке установки Kaspersky Security Center. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Вам нужно запустить утилиту klsrvswch на устройстве Сервера администрирования под учетной записью с правами администратора, которая использовалась для установки Сервера администрирования.

2. Нажимайте на кнопку **Далее** мастера, пока не дойдете до шага **Изменить учетные данные для доступа к СУБД**.

3. На шаге мастера **Изменить учетные данные для доступа к СУБД** выполните следующие действия:

   Шаг мастера **Изменить учетные данные для доступа к СУБД** пропускается, если используется аутентификация Windows.

   - Выберите параметр **Применить новые учетные данные**.
   - Укажите новое имя учетной записи в поле **Учетная запись**.
   - Укажите новый пароль для учетной записи в поле **Пароль**.
   - Подтвердите новый пароль в поле **Подтвердить пароль**.

   Вам нужно указать учетные данные учетной записи, которая существует в СУБД.

4. Нажмите на кнопку **Далее**.

После завершения работы мастера учетные данные СУБД изменяются.

Утилиту klsrvswch можно использовать только для изменения пароля учетной записи для аутентификации SQL. Изменение способа авторизации не поддерживается. Для изменения способа авторизации переустановите Сервер администрирования и укажите нужные параметры.

Изменение общей папки Сервера администрирования

Общая папка Сервера администрирования указывается при установке Сервера администрирования. Месторасположение папки общего доступа можно изменить в свойствах Сервера администрирования.

Чтобы изменить общую папку:

1. Создайте сетевую папку общего доступа и настройте разрешения для общей папки и для структуры папок, чтобы предоставить права полного контроля для подгруппы **Everyone**.
2. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
3. В окне свойства Сервера администрирования в панели **Разделы** перейдите в раздел **Дополнительно** и выберите **Папка общего доступа Сервера администрирования**.
4. В разделе **Папка общего доступа Сервера администрирования** нажмите на кнопку **Изменить**.
5. Выберите папку, которую вы хотите использовать как общую.
6. Нажмите на кнопку **OK**, чтобы закрыть окно свойств Сервера администрирования.
7. Назначить права на чтение для подгруппы **Everyone** для папки, которую вы выбрали как общую.

Решение проблем с узлами Сервера администрирования

Дерево в левой панели Консоли администрирования содержит узлы, соответствующие Серверам администрирования. Вы можете добавить в дерево консоли столько Серверов администрирования, сколько вам нужно.

Консоль управления Microsoft Management Console (MMC) сохраняет список узлов Сервера администрирования в дереве консоли в теневую копию файла .msc. Теневая копия этого файла хранится в папке %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ на устройстве, на котором установлена Консоль администрирования. Для каждого узла Сервера администрирования в файле содержится следующая информация:

- Адрес Сервера администрирования.
- Номер порта
- Используется ли TLS

  Этот параметр зависит от номера порта, используемого для подключения Консоли администрирования к Серверу администрирования.

- Имя пользователя.
- Сертификат Сервера администрирования.

Устранение неисправностей

При подключении Консоли администрирования к Серверу администрирования сохраненный локально сертификат сравнивается с сертификатом Сервера администрирования. Если сертификаты не совпадают, в Консоли администрирования возникает ошибка. Несовпадение сертификатов может произойти, например, при замене сертификата Сервера администрирования. В этом случае необходимо повторно создать узел Сервер администрирования в консоли.

Чтобы повторно создать узел Сервера администрирования:

1. Закройте окно Консоли администрирования Kaspersky Security Center.
2. Удалите файл Kaspersky Security Center 15.1 из папки %USERPROFILE%\AppData\Roaming\Microsoft\MMC\.
3. Запустить Консоль администрирования Kaspersky Security Center.

   Отобразится предложение подключиться к Серверу администрирования и принять его существующий сертификат.
4. Выполните одно из следующих действий:
   - Примите существующий сертификат, нажав на кнопку **Да**.
   - Чтобы указать ваш сертификат, нажмите на кнопку **Нет** и перейдите к файлу сертификата, используемого для аутентификации Сервера администрирования.

Проблема с сертификатом решена. Вы можете использовать Консоль администрирования для подключения к Серверу администрирования.

Просмотр и изменение параметров Сервера администрирования

Вы можете настраивать параметры Сервера администрирования в окне свойств Сервера администрирования.

Чтобы открыть окно Свойства: Сервер администрирования,

в контекстном меню узла Сервера администрирования в дереве консоли выберите пункт **Свойства**.

Настройка общих параметров Сервера администрирования

Вы можете настраивать общие параметры Сервера администрирования в разделах **Общие**, **Параметры подключения к Серверу администрирования**, **Хранилище событий** и **Безопасность** окна свойств Сервера администрирования.

Раздел **Безопасность** не отображается в окне свойств Сервера администрирования, если его отображение выключено в интерфейсе Консоли администрирования.

*Чтобы включить отображение раздела **Безопасность** в Консоли администрирования:*

1. В дереве консоли выберите требуемый Сервер администрирования.
2. В меню **Вид** главного окна приложения выберите пункт **Настройка интерфейса**.
3. В открывшемся окне **Настройка интерфейса** установите флажок **Отображать разделы с параметрами безопасности** и нажмите на кнопку **OK**.
4. В окне с сообщением приложения нажмите на кнопку **OK**.

Раздел **Безопасность** отобразится в окне свойств Сервера администрирования.

Параметры интерфейса Консоли администрирования

Вы можете настроить параметры интерфейса Консоли администрирования для отображения или скрытия элементов управления пользовательского интерфейса, связанных со следующими функциями:

- Системное администрирование.
- Шифрование и защита данных.
- Параметры контроля рабочего места.
- Управление мобильными устройствами.
- Подчиненные Серверы администрирования.
- Разделы с параметрами безопасности.

Чтобы настроить параметры интерфейса Консоли администрирования:

1. В дереве консоли выберите требуемый Сервер администрирования.
2. В меню **Вид** главного окна приложения выберите пункт **Настройка интерфейса**.
3. В открывшемся окне **Настройка интерфейса** установите флажок рядом с функциональностью, которая должна отображаться, и нажмите на кнопку **OK**.
4. В окне с сообщением приложения нажмите на кнопку **OK**.

Выбранная функциональность отображается в интерфейсе Консоли администрирования.

Обработка и хранение событий на Сервере администрирования

Информация о событиях, возникших в работе приложения и управляемых устройств, сохраняется в базе данных Сервера администрирования. Каждое событие относится к определенному типу и уровню важности (*Критическое событие*, *Отказ функционирования*, *Предупреждение*, *Информационное сообщение*). В зависимости от условий, при которых произошло событие, приложение может присваивать событиям одного типа разные уровни важности.

Вы можете просматривать типы и уровни важности событий в разделе **Настройка событий** окна свойств Сервера администрирования. В разделе **Настройка событий** вы также можете настроить параметры обработки каждого события Сервером администрирования:

- регистрацию событий на Сервере администрирования и в журналах событий операционной системы на устройстве и на Сервере администрирования;
- способ уведомления администратора о событии (например, SMS, сообщение электронной почты).

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, приложение вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400 000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Приложение проверяет базу данных каждые 10 минут. Если количество событий достигает на 10 000 больше указанного максимального значения, приложение удаляет самые старые события, чтобы осталось только указанное максимальное количество событий.

Когда Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий Kaspersky Event Log. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления.

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.

Просмотр журнала подключений к Серверу администрирования

Можно сохранить в файл журнала историю подключений и попыток подключения к Серверу администрирования в процессе его работы. Информация в файле позволит отследить не только подключения внутри инфраструктуры сети, но и попытки несанкционированного доступа к Серверу администрирования.

Чтобы настроить регистрацию событий подключения к Серверу администрирования:

1. В дереве консоли выберите Сервер администрирования, для которого нужно включить регистрацию событий подключения.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В открывшемся окне свойств в разделе **Параметры подключения к Серверу администрирования** выберите вложенный раздел **Порты подключения**.
4. Включите параметр **Записывать события соединения с Сервером администрирования в журнал**.
5. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств Сервера администрирования.

Все последующие события входящих подключений к Серверу администрирования, результаты аутентификации и ошибки SSL будут записываться в файл %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog.

Контроль возникновения вирусных эпидемий

Kaspersky Security Center позволяет вам своевременно реагировать на возникновение угроз вирусных атак. Оценка угрозы вирусной эпидемии производится путем контроля вирусной активности на устройствах.

Вы можете настраивать правила оценки угрозы вирусной эпидемии и действия в случае ее возникновения в разделе **Вирусная атака** окна свойств Сервера администрирования.

Порядок оповещения о событии *Вирусная атака* можно задать в разделе **Настройка событий** окна свойств Сервера администрирования, в окне свойств события *Вирусная атака*.

Событие *Вирусная атака* формируется при возникновении событий *Обнаружен вредоносный объект* в работе приложений безопасности. Поэтому для распознавания вирусной эпидемии информацию о событиях *Обнаружен вредоносный объект* требуется сохранять на Сервере администрирования.

Параметры сохранения информации о событии *Обнаружен вредоносный объект* задаются в политиках приложений безопасности.

> При подсчете событий *Обнаружен вредоносный объект* учитывается только информация с устройств главного Сервера администрирования. Информация с подчиненных Серверов администрирования не учитывается. Для каждого подчиненного Сервера параметры события *Вирусная атака* требуется настраивать индивидуально.

Ограничение трафика

Для уменьшения объемов трафика в сети приложение предоставляет возможность ограничить скорость передачи данных на Сервер администрирования с заданных IP-диапазонов и IP-подсетей.

Вы можете создавать и настраивать правила ограничения трафика в разделе **Трафик** окна свойств Сервера администрирования.

Чтобы создать правило ограничения трафика:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования, для которого нужно создать правила ограничения трафика.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Трафик**.
4. Нажмите на кнопку **Добавить**.
5. В разделе **Новое правило** укажите следующие параметры:

   В блоке **Интервал IP-адресов, для которых нужно ограничивать трафик** можно выбрать способ задания подсети или диапазона, для которого ограничивается скорость передачи, и указать значения параметров для выбранного способа. Выберите один из следующих способов:

   - **Задать интервал адресом и маской подсети**

     Трафик ограничен в соответствии с параметрами подсети. Укажите в полях ввода адрес подсети и маску подсети для определения интервала, в пределах которого будет ограничен трафик.

Вы также можете нажать на кнопку **Обзор**, чтобы добавить подсети из глобального списка подсетей.

- **Задать интервал начальным и конечным IP-адресом**

  Трафик ограничивается по интервалу IP-адресов. Укажите интервал IP-адресов в полях ввода **Начальный IP-адрес** и **Конечный IP-адрес**.

  Этот вариант выбран по умолчанию.

В блоке **Ограничение трафика** можно настроить следующие параметры ограничения скорости передачи данных:

- **Период**

  Временной интервал, во время которого будет действовать ограничение трафика. Границы временного интервала можно указать в полях ввода.

- **Ограничение (КБ/сек)**

  Предельное значение суммарной скорости передачи входящих и исходящих данных Сервера администрирования. Ограничение действует только в течение временного интервала, заданного в поле **Период**.

- **Ограничивать трафик на оставшееся время (КБ/сек)**

  Трафик ограничивается не только в течение интервала, указанного в поле **Период**, но и в остальное время.

  По умолчанию флажок снят. Значение поля может не совпадать со значением поля **Ограничение (КБ/сек)**.

В первую очередь правила ограничения трафика влияют на передачу файлов. Эти правила не применяются к трафику, который возникает при синхронизации между Сервером администрирования и Агентом администрирования, или между главным Сервером администрирования и подчиненным Сервером администрирования.

Настройка параметров Веб-сервера

Веб-сервер используется для публикации автономных инсталляционных пакетов, iOS MDM-профилей, а также файлов из папки общего доступа.

Вы можете настроить параметры подключения Веб-сервера к Серверу администрирования и задать сертификат Веб-сервера в разделе **Веб-сервер** окна свойств Сервера администрирования.

Работа с внутренними пользователями

Учетные записи *внутренних пользователей* используются для работы с виртуальными Серверами администрирования. Kaspersky Security Center внутренние пользователи обладают правами реальных пользователей.

Учетные записи внутренних пользователей создаются и используются только внутри Kaspersky Security Center. Сведения о внутренних пользователях не передаются операционной системе. Аутентификацию внутренних пользователей осуществляет Kaspersky Security Center.

Вы можете настраивать параметры учетных записей внутренних пользователей в папке **Учетные записи пользователей** дерева консоли.

Резервное копирование и восстановление параметров Сервера администрирования

Для резервного копирования параметров Сервера администрирования и используемой им базы данных предусмотрены задача резервного копирования и утилита klbackup. Резервная копия включает в себя все основные параметры и объекты Сервера администрирования: сертификаты Сервера администрирования, мастер-ключи шифрования дисков управляемых устройств, ключи для лицензий, структуру групп администрирования со всем содержимым, задачи, политики и так далее. Имея резервную копию, можно восстановить работу Сервера администрирования в кратчайшие сроки – от десятков минут до двух часов.

В случае отсутствия резервной копии сбой может привести к безвозвратной потере сертификатов и всех параметров Сервера администрирования. Это повлечет необходимость заново настраивать Kaspersky Security Center, а также заново выполнять первоначальное развертывание Агента администрирования в сети организации. Кроме того, будут потеряны и мастер-ключи шифрования дисков управляемых устройств, что создаст риск безвозвратной потери зашифрованных данных на устройствах с Kaspersky Endpoint Security. Поэтому не следует отказываться от регулярного создания резервных копий Сервера администрирования с помощью штатной задачи резервного копирования.

Мастер первоначальной настройки приложения создает задачу резервного копирования параметров Сервера администрирования с ежедневным запуском в четыре часа ночи. Резервные копии по умолчанию сохраняются в папке %ALLUSERSPROFILE%\Application Data\KasperskySC.

Если в качестве СУБД используется экземпляр Microsoft SQL Server, установленный на другом устройстве, следует изменить задачу резервного копирования: указать в качестве папки для хранения сделанных резервных копий UNC-путь, доступный на запись как службе Сервера администрирования, так и службе SQL Server. Это требование является следствием особенности резервного копирования в СУБД Microsoft SQL Server.

Если в качестве СУБД используется локальный экземпляр Microsoft SQL Server, также рекомендуется сохранять резервные копии на отдельном носителе, чтобы обезопасить их от повреждения одновременно с Сервером администрирования.

Поскольку резервная копия содержит важные данные, в задаче резервного копирования и в утилите klbackup предусмотрена защита резервных копий паролем. По умолчанию задача резервного копирования создается с пустым паролем. Следует обязательно задать пароль в свойствах задачи резервного копирования. Несоблюдение этого требования приведет к тому, что ключи сертификатов Сервера администрирования, ключи для лицензий и мастер-ключи шифрования дисков управляемых устройств окажутся незашифрованными.

Помимо регулярного резервного копирования, следует также создавать резервную копию перед всеми значимыми изменениями, в том числе перед обновлением Сервера администрирования до новой версии и перед установкой патчей Сервера администрирования.

Если вы используете Microsoft SQL Server в качестве СУБД, вы можете минимизировать размер резервных копий. Для этого установите флажок **Сжимать резервные копии (Compress backup)** в параметрах SQL Server.

Восстановление из резервной копии выполняется с помощью утилиты klbackup на только что установленном и работоспособном экземпляре Сервера администрирования той версии, для которой была сделана резервная копия (или более новой).

Экземпляр Сервера администрирования, на который выполняется восстановление, должен использовать СУБД того же типа (например, тот же SQL Server или MariaDB) той же самой или более новой версии. Версия Сервера администрирования может быть той же самой (с аналогичным или более новым патчем) или более новой.

В этом разделе описаны типовые сценарии восстановления параметров и объектов Сервера администрирования.

Использование снимка файловой системы для уменьшения времени резервного копирования

В Kaspersky Security Center 15.1 уменьшено по сравнению с более ранними версиями время простоя Сервера администрирования во время резервного копирования данных. Кроме того, в параметры задачи добавлена функция **Использовать моментальный снимок файловой системы для резервного копирования данных**. Эта функция позволяет дополнительно уменьшить время простоя за счет того, что утилита klbackup создает при выполнении резервного копирования теневую копию диска (это занимает несколько секунд) и одновременно производит копирование базы данных (это занимает не более нескольких минут). Создав теневую копию диска и сделав копию базы данных, klbackup снова делает Сервер администрирования доступным для соединения.

Вы можете пользоваться функцией создания снимка файловой системы только при соблюдении двух условий:

- Папка общего доступа Сервера администрирования и папка %ALLUSERSPROFILE%\KasperskyLab находятся на одном логическом диске и локальны по отношению к Серверу администрирования.
- Внутри папки %ALLUSERSPROFILE%\KasperskyLab нет созданных вручную символических ссылок.

Не используйте функцию, если хотя бы одно из этих условий не выполняется. В ответ на попытку создать снимок файловой системы приложение выдаст сообщение об ошибке.

Для использования функции необходимо иметь учетную запись с правами на создание снимков логического диска, на котором расположена папка %ALLUSERSPROFILE%. Учетная запись службы сервера администрирования не имеет таких прав.

Чтобы воспользоваться функцией создания снимка файловой системы для уменьшения времени резервного копирования:

1. В разделе **Задачи** выберите задачу резервного копирования.
2. В контекстном меню выберите пункт **Свойства**.
3. В отобразившемся окне свойств задачи выберите раздел **Параметры**.
4. Установите флажок **Использовать моментальный снимок файловой системы для резервного копирования данных**.
5. В полях **Имя пользователя** и **Пароль** введите имя и пароль от учетной записи, имеющей право на создание снимков логического диска, на котором расположена папка %ALLUSERSPROFILE%.
6. Нажмите на кнопку **Применить**.

При следующих запусках задачи резервного копирования утилита klbackup будет создавать снимки файловой системы, и время простоя Сервера администрирования во время выполнения задачи уменьшится.

Вышло из строя устройство с Сервером администрирования

Если в результате сбоя вышло из строя устройство с Сервером администрирования, рекомендуется выполнить следующие действия:

- Новому Серверу назначить тот же самый адрес: NetBIOS-имя, FQDN-имя, статический IP – в зависимости от того, что было задано при развертывании Агентов администрирования.
- Установить Сервер администрирования с использованием СУБД того же типа, той же или более новой версии. Можно установить ту же версию Сервера с тем же или более новым патчем, или более новую версию. После установки не следует выполнять первоначальную настройку с помощью мастера.
- Из меню **Пуск** запустить утилиту резервного копирования klbackup и выполнить восстановление.

Повреждены параметры Сервера администрирования или база данных

Если Сервер администрирования стал неработоспособен в результате повреждения параметров или базы данных (например, из-за сбоя питания), рекомендуется использовать следующий сценарий восстановления:

1. Выполнить проверку файловой системы на пострадавшем устройстве.
2. Деинсталлировать неработоспособную версию Сервера администрирования.
3. Заново установить Сервер администрирования с использованием СУБД того же типа, той же или более новой версии. Можно установить ту же версию Сервера с тем же или более новым патчем, или более новую версию. После установки не следует выполнять первоначальную настройку с помощью мастера.
4. Из меню **Пуск** запустить утилиту резервного копирования klbackup и выполнить восстановление.

Недопустимо восстанавливать Сервер администрирования любым другим способом, кроме штатной утилиты klbackup.

Во всех случаях восстановления Сервера с помощью стороннего программного обеспечения неизбежно произойдет рассинхронизация данных на узлах распределенного приложения Kaspersky Security Center и, как следствие, неправильная работа приложения.

Резервное копирование и восстановление данных Сервера администрирования

Резервное копирование данных позволяет переносить Сервер администрирования с одного устройства на другое без потерь информации. С помощью резервного копирования вы можете восстанавливать данные при переносе информационной базы Сервера администрирования на другое устройство или при переходе на более позднюю версию Kaspersky Security Center. Также вы можете использовать резервное копирование данных для переноса данных Сервера администрирования Kaspersky Security Center Windows под управление Kaspersky Security Center Linux (перенос данных из Kaspersky Security Center Linux в Kaspersky Security Center Windows не поддерживается).

Резервные копии установленных плагинов управления не сохраняются. После восстановления данных Сервера администрирования из резервной копии необходимо загрузить и переустановить плагины управляемых приложений.

Прежде чем создавать резервную копию данных Сервера администрирования, проверьте, добавлен ли виртуальный Сервер администрирования в группу администрирования. Если виртуальный Сервер администрирования добавляется перед резервным копированием, убедитесь, что этому виртуальному Серверу назначен администратор. Вы не можете предоставить права администратора к виртуальному Серверу администрирования после резервного копирования. Обратите внимание, если учетные данные администратора утеряны, вы не сможете назначить нового администратора виртуальному Серверу администратора.

Для резервного копирования или восстановления отказоустойчивого кластера Kaspersky Security Center нужно остановить весь кластер для обслуживания, а затем перезагрузить его после завершения резервного копирования или восстановления.

Вы можете создать резервную копию данных Сервера администрирования одним из следующих способов:

- Создать и запустить задачу резервного копирования данных через Консоль администрирования.
- Запустить утилиту klbackup на устройстве, где установлен Сервер администрирования. Утилита входит в состав комплекта поставки Kaspersky Security Center. После установки Сервера администрирования утилита находится в корне папки назначения, указанной при установке приложения.

В резервной копии данных Сервера администрирования сохраняются следующие данные:

- база данных Сервера администрирования (политики, задачи, параметры приложений, сохраненные на Сервере администрирования события);
- конфигурационная информация о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов приложений для удаленной установки;
- сертификат Сервера администрирования;

- Содержимое папки *Обновления*.

  По умолчанию путь к папке – C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\

Восстановление данных Сервера администрирования возможно только с помощью утилиты klbackup. Вам нужно выполнить восстановление на только что установленном и работоспособном экземпляре Сервера администрирования той версии, для которой была сделана резервная копия (или более новой).

Задача Резервное копирование данных Сервера администрирования

Создание задачи Резервное копирование данных Сервера администрирования

Задача резервного копирования – это задача Сервера администрирования; она создается с помощью мастера первоначальной настройки. Если задача резервного копирования, созданная мастером первоначальной настройки, была удалена, вы можете создать ее вручную.

Чтобы создать задачу Резервное копирование данных Сервера администрирования:

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания одним из следующих способов:
   - В контекстном меню папки дерева консоли **Задачи** выберите пункт **Создать → Задачу**.
   - Нажмите на кнопку **Создать задачу**, расположенную в рабочей области.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера. В окне мастера **Выбор типа задачи** выберите тип задачи **Резервное копирование данных Сервера администрирования**.

Задачу **Резервное копирование данных Сервера администрирования** можно создать только в одном экземпляре. Если задача резервного копирования данных Сервера администрирования уже создана для Сервера администрирования, то она не отображается в окне выбора типа задачи мастера создания задачи резервного копирования.

Настройка задачи Резервное копирование данных Сервера администрирования

После создания задачи резервного копирования вы можете настроить параметры задачи.

Чтобы настроить параметры задачи Резервное копирование данных Сервера администрирования:

1. В дереве консоли выберите папку **Задачи**.
2. В контекстном меню задачи **Резервное копирование данных Сервера администрирования** выберите пункт **Свойства**.

Откроется окно свойств задачи *Резервное копирование данных Сервера администрирования*. Доступны следующие свойства:

- **Общие**

  В разделе **Общие** вы можете указать название задачи, просмотреть дату создания задачи, дату последней команды, статусы запуска задачи и результаты выполнения задачи.

- **Уведомление**

  В разделе **Уведомление** вы можете указать параметры хранения событий, связанных с результатами выполнения задачи и настроить уведомления о результатах выполнения задачи.

- **Расписание**

  В разделе **Расписание** вы можете указать расписание запуска задачи.

- **Назначение**

  В разделе **Назначение** вы можете указать путь к папке, в которой будут храниться резервные копии данных Сервера администрирования.

- **Параметры**

  В разделе **Параметры** вы можете установить защиту паролем резервных копий данных и количество резервных копий, если это необходимо.

  Вы также можете создать теневую копию логического диска с папкой% ALLUSERSPROFILE% и скопировать базу данных Сервера администрирования. Для этого необходимо включить параметр **Использовать моментальный снимок файловой системы для резервного копирования данных** и указать имя и пароль учетной записи, у которой есть разрешение на создание моментальных снимков.

- **Безопасность**

  В разделе **Безопасность** вы можете предоставить пользователям и группам права на выполнение операций на Сервере администрирования. Если включен параметр **Наследовать параметры Сервера администрирования**, параметры безопасности задачи наследуются от Сервера администрирования.

  Если этот параметр выключен, вы можете настроить параметры задачи. Вы можете назначить роль пользователю или группе пользователей или назначить права пользователю или группе пользователей, применительно к задаче.

  По умолчанию параметр **Наследовать параметры Сервера администрирования** включен.

- **История ревизий**

  В разделе **История ревизий** вы можете контролировать изменения задачи. Каждый раз, когда вы сохраняете изменения задачи, создается ревизия.

Утилита резервного копирования и восстановления данных (klbackup)

Вы можете выполнять копирование данных Сервера администрирования для резервного хранения и последующего восстановления с помощью утилиты klbackup, входящей в состав дистрибутива Kaspersky Security Center.

Утилита klbackup может работать в двух режимах:

- интерактивный;
- тихий.

Резервное копирование и восстановление данных в интерактивном режиме

Чтобы создать резервную копию данных Сервера администрирования в интерактивном режиме:

1. Запустите утилиту klbackup, расположенную в папке установки Kaspersky Security Center.

   В результате запустится мастер выполнения резервного копирования и восстановления данных.

2. В первом окне мастера выберите **Выполнить резервное копирование данных Сервера администрирования**.

   При выборе параметра **Выполнять резервное копирование и восстановление только для сертификата Сервера администрирования** будут сохранены только резервная копия сертификата Сервера администрирования и закрытый ключ. Резервное копирование сертификата и закрытого ключа Сервера администрирования может быть полезно при выполнении переноса данных с Сервера администрирования Kaspersky Security Center Windows на Сервер администрирования Kaspersky Security Center Linux. Также вы можете переносить управляемые устройства между Серверами администрирования Kaspersky Security Center Linux и между Серверами администрирования Kaspersky Security Center Windows. Подробнее см. Использование утилиты klbackup для переключения управляемых устройств под управление другого Сервера администрирования.

   Нажмите **Далее**.

3. В следующем окне мастера укажите параметры:

   - **Папка назначения резервного копирования**
   - **Перенести данные базы данных**

     Включите этот параметр, если в настоящее время вы храните данные Сервера администрирования в базе данных Microsoft SQL Server и вам нужно перенести их в одну из следующих баз данных: MySQL или MariaDB, PostgreSQL или Postgres Pro, Azure SQL. По умолчанию параметр выключен.

     - **Перенос данных в формате MySQL/MariaDB**

       Включите этот параметр, если в настоящее время вы используете SQL Server в качестве СУБД для Сервера администрирования и хотите перенести данные с SQL Server на MySQL или MariaDB. Kaspersky Security Center создаст резервную копию данных, совместимую с MySQL и MariaDB. После этого вы можете восстановить данные из резервной копии в MySQL или MariaDB.

     - **Перенос данных в Postgres**

       Включите этот параметр, если в качестве СУБД для Сервера администрирования используется SQL Server и требуется перенести данные из SQL Server в СУБД PostgreSQL или Postgres Pro. Kaspersky Security Center создаст резервную копию данных, совместимую с PostgreSQL и Postgres Pro. После этого можно будет восстановить данные из этой резервной копии в PostgreSQL или Postgres Pro.

       Этот параметр становится доступным, если вы обновляете Kaspersky Security Center Windows до версии 15.1.0.28509.

- **Перенести в формат Azure**

  Включите этот параметр, если в настоящее время вы используете SQL Server в качестве СУБД для Сервера администрирования и хотите перенести данные из SQL Server в Azure SQL. Kaspersky Security Center создаст резервную копию данных, совместимую с Azure SQL. После этого вы можете восстановить данные из резервной копии в Azure SQL.

- **Включать текущую дату и время в имя папки назначения для резервных копий**

- **Пароль для резервной копии данных**

4. Нажмите на кнопку **Далее** для выполнения резервного копирования.

5. Если вы работаете с базой данных в облачном окружении, таком как Amazon Web Services (AWS) или Microsoft Azure, заполните следующие поля в окне **Войти в онлайн-хранилище**:

   - Для AWS:

     - **Имя корзины S3**

       Имя корзины S3, которое вы создали для резервной копии данных.

     - **ID ключа доступа**

       Вы получили ID ключа (последовательность из букв и цифр), когда создали учетную запись IAM-пользователя для работы с корзиной S3 в хранилище инстансов.

       Поле доступно, если вы выбрали базу RDS для контейнера S3.

     - **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, а не IAM-роль.

   - Для Microsoft Azure:

     - **Имя учетной записи хранения Azure**

       Вы создали имя учетной записи хранения Azure для работы с Kaspersky Security Center.

     - **Идентификатор подписки Azure**

       Вы создали подписку на портале Azure.

     - **Пароль 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.

     - **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.

- **Имя SQL-сервера Azure**

  Имя и группа источника доступны в свойствах SQL-сервера Azure.

- **Группа источника SQL-сервера Azure**

  Имя и группа источника доступны в свойствах SQL-сервера Azure.

- **Ключ доступа хранилища Azure**

  Доступен в свойствах учетной записи хранения в разделе "Access Keys". Вы можете использовать любой ключ (key1 или key2).

Чтобы восстановить данные Сервера администрирования в интерактивном режиме:

1. Запустите утилиту klbackup, расположенную в папке установки Kaspersky Security Center. Запустите утилиту под той же учетной записью, под которой был установлен Сервер администрирования. Рекомендуется запускать утилиту на только что установленном Сервере администрирования.

   В результате запустится мастер выполнения резервного копирования и восстановления данных.

2. В первом окне мастера выберите **Выполнить восстановление данных Сервера администрирования** и нажмите на кнопку **Далее**.

   Если вы выбрали параметр **Выполнять резервное копирование и восстановление только для сертификата Сервера администрирования**, будет выполнено только восстановление сертификата Сервера администрирования и закрытого ключа.

   При запуске утилиты klbackup на неактивном узле отказоустойчивого кластера вам будет предложено выбрать один из вариантов: указать сертификат Сервера администрирования или автоматически получать данные с Сервера администрирования.

3. В окне мастера **Параметры восстановления**:

   - Укажите папку, содержащую резервную копию данных Сервера администрирования.

     Если вы работаете в облачном окружении, таком как AWS или Azure, укажите адрес хранилища. Также убедитесь, что файл называется backup.zip.

   - Укажите пароль, введенный при резервном копировании данных.

     При восстановлении данных необходимо указать тот же пароль, который был введен во время резервного копирования. Если после резервного копирования путь к общей папке изменился, проверьте работу задач, использующих восстановленные данные (задачи восстановления и задачи удаленной установки). При необходимости отредактируйте параметры этих задач. Пока данные восстанавливаются из файла резервной копии, никто не должен иметь доступ к общей папке Сервера администрирования. Учетная запись, под которой запускается утилита klbackup, должна иметь полный доступ к общей папке.

4. Нажмите на кнопку **Далее** для восстановления данных.

Резервное копирование и восстановление данных в тихом режиме

Чтобы создать резервную копию данных или восстановить данные Сервера администрирования в тихом режиме,

в командной строке устройства, на котором установлен Сервер администрирования, запустите утилиту klbackup с необходимым набором ключей.

При использовании утилиты klbackup флаги Агента администрирования не восстанавливаются. Вам необходимо вручную настроить флаги Агента администрирования.

Экземпляр Сервера администрирования, на который выполняется восстановление, должен использовать СУБД того же типа. Версия Сервера администрирования может быть той же самой (с аналогичным или более новым патчем) или более новой.

Синтаксис командной строки утилиты:

```
klbackup -path <путь к резервной копии> [-linux_path <путь к резервной копии SQL Server>][-node_cert <путь к сертификату>] [-logfile <файл журнала>] [-use_ts]|[-restore] [-password <пароль>] [-cert_only] [-online] [-migrate postgres]
```

Если не задать пароль в командной строке утилиты klbackup, утилита запросит его ввод интерактивно.

Описания ключей:

- `-path <путь к резервной копии>` – сохранять информацию в указанной папке резервной копии или использовать для восстановления данные из папки к резервной копии (обязательный параметр).

  Учетная запись сервера базы данных и утилита klbackup должны обладать правами на изменение данных в папке резервной копии.

- `-linux_path <путь к резервной копии SQL Server>` – локальный путь к папке с резервной копией данных для SQL Server для Linux.

  Учетная запись сервера базы данных и утилита klbackup должны обладать правами на изменение данных в папке резервной копии SQL Server.

- `-node_cert <путь к сертификату>` – файл сертификата Сервера для настройки пассивного узла отказоустойчивого кластера после восстановления. Если параметр не указан, он будет автоматически получен с Сервера.

  При запуске утилиты klbackup на неактивном узле отказоустойчивого кластера используйте этот ключ, чтобы указать путь к сертификату Сервера администрирования.

- `-logfile <файл журнала>` – сохранять отчет о копировании или восстановлении данных Сервера администрирования.

- `-use_ts` – при сохранении данных копировать информацию в папку резервной копии, во вложенную папку с именем в формате `klbackup ГГГГ-ММ-ДД # ЧЧ-ММ-СС`, включающем текущие дату и время операции в формате UTC. Если ключ не задан, информация сохраняется в корне папки резервной копии.

  При попытке сохранить информацию в папку, в которой уже есть резервная копия, появится сообщение об ошибке. Обновление информации не произойдет.

Наличие ключа `-use_ts` позволяет вести архив данных Сервера администрирования. Например, если ключом `-path` была задана папка `C:\KLBackups`, то в папке `klbackup 2022-06-19 # 11-30-18`, сохранится информация о состоянии Сервера администрирования на дату 19 июня 2022 года, 11 часов 30 минут 18 секунд.

- `-restore` – выполнить восстановление данных Сервера администрирования. Восстановление данных осуществляется на основании информации, представленной в папке резервной копии. Если ключ отсутствует, производится резервное копирование данных в папку резервной копии.

- `-password <пароль>` – пароль для защиты конфиденциальных данных.

  Забытый пароль не может быть восстановлен. Требования к паролю отсутствуют. Длина пароля не ограничена, также возможна нулевая длина пароля (то есть без пароля).

  При восстановлении данных необходимо указать тот же пароль, который был введен во время резервного копирования. Если после резервного копирования путь к общей папке изменился, проверьте работу задач, использующих восстановленные данные (задачи восстановления и задачи удаленной установки). При необходимости отредактируйте параметры этих задач. Пока данные восстанавливаются из файла резервной копии, никто не должен иметь доступ к общей папке Сервера администрирования. Учетная запись, под которой запускается утилита klbackup, должна иметь полный доступ к общей папке. Рекомендуется запускать утилиту на только что установленном Сервере администрирования.

- `-cert_only` – сохранить или восстановить только сертификат и закрытый ключ Сервера администрирования.

  Этот флаг может быть полезен при выполнении переноса данных с Сервера администрирования Kaspersky Security Center Windows на Сервер администрирования Kaspersky Security Center Linux. Также вы можете переносить управляемые устройства между Серверами администрирования Kaspersky Security Center Linux и между Серверами администрирования Kaspersky Security Center Windows.

- `-online` – создать резервную копию данных Сервера администрирования, создав моментальный снимок, чтобы минимизировать время автономного состояния Сервера администрирования. Если вы используете утилиту резервного копирования и восстановления данных, этот параметр игнорируется. Не используйте этот флаг при создании резервной копии для перехода на другую СУБД.

- `- archive 0` – хранить данные сервера в виде простых файлов. По умолчанию (`-archive 1`) данные сервера хранятся в архивном файле.

- `-migrate mysql` – создание резервной копии данных Сервера администрирования, хранящихся в базе данных SQL Server, совместимой с MySQL (включая MariaDB). Данные из этой резервной копии можно восстановить в MySQL.

- `-migrate postgres` – создание резервной копии данных Сервера администрирования, хранящихся в базе данных SQL Server, совместимой с PostgreSQL и Postgres Pro. Данные из этой резервной копии можно восстановить в PostgreSQL или Postgres Pro. Этот флаг используется при выполнении переноса данных в Kaspersky Security Center Linux с использованием резервной копии данных Сервера администрирования.

  Этот параметр становится доступным, если вы обновляете Kaspersky Security Center Windows до версии 15.1.0.28509.

Использование утилиты klbackup для переключения управляемых устройств под управление другого Сервера администрирования

Утилита klbackup позволяет переключать управляемые устройства под управление другого Сервера администрирования. Вы можете сменить Сервер администрирования Kaspersky Security Center Windows на Сервер администрирования Kaspersky Security Center Linux, используя утилиту klbackup, при выполнении переноса данных. Также вы можете переносить управляемые устройства между Серверами администрирования Kaspersky Security Center Linux и между Серверами администрирования Kaspersky Security Center Windows.

Чтобы переключить управляемые устройства под управление другого Сервера администрирования с помощью утилиты klbackup:

1. На предыдущем устройстве создайте резервную копию сертификата и закрытого ключа Сервера администрирования.

   Вы можете создать резервную копию данных одним из следующих способов:

   - С помощью интерфейса утилиты klbackup (только для Сервера администрирования Kaspersky Security Center Windows).

     Запустите утилиту klbackup, расположенную в папке установки Kaspersky Security Center, а затем создайте резервную копию с помощью параметра **Выполнять резервное копирование и восстановление только для сертификата Сервера администрирования**.

   - С помощью командной строки (для Серверов администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux версии 15.1 и выше).

     Запустите утилиту klbackup с ключом `-cert_only` из командной строки, чтобы создать резервную копию сертификата и закрытого ключа Сервера администрирования:

     ```
     klbackup -path <путь к резервной копии сертификата Сервера администрирования> -cert_only
     ```

2. На предыдущем устройстве отключите Сервер администрирования от сети.

3. Назначьте устройству с другим Сервером администрирования тот же адрес.

   Новому Серверу администрирования можно присвоить имя NetBIOS, FQDN и статический IP-адрес. Это зависит от того, какой адрес Сервера администрирования был установлен в инсталляционном пакете Агента администрирования, когда были развернуты Агенты администрирования. Также вы можете использовать адрес подключения, определяющий Сервер администрирования, к которому подключается Агент администрирования (вы можете получить этот адрес на управляемых устройствах с помощью утилиты klnagchk).

4. На устройстве с другим Сервером администрирования восстановите сертификат Сервера администрирования и закрытый ключ из резервной копии.

   Вы можете восстановить резервную копию данных одним из следующих способов:

   - С помощью интерфейса утилиты klbackup (только для Сервера администрирования Kaspersky Security Center Windows).

     Запустите утилиту klbackup и восстановите резервную копию, используя параметр **Выполнять резервное копирование и восстановление только для сертификата Сервера администрирования**.

   - С помощью командной строки (для Серверов администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux версии 15.1 и выше).

Запустите утилиту klbackup с ключом `-cert_only` из командной строки, чтобы восстановить резервную копию сертификата и закрытого ключа Сервера администрирования:

```
klbackup -path <путь к резервной копии сертификата Сервера администрирования> -restore -cert_only
```

Управляемые устройства перейдут под управление другого Сервера администрирования. Вы можете перейти на Сервер администрирования и убедиться, что управляемые устройства видны в сети и что на них установлен и запущен Агент администрирования (значение *Да* в столбцах **Видимо в сети**, **Агент администрирования установлен** и **Агент администрирования запущен**).

Резервное копирование и восстановление данных Сервера администрирования при использовании MySQL или MariaDB

Вы можете использовать резервное копирование данных, чтобы перенести данные Сервера администрирования из Kaspersky Security Center Windows под управление Kaspersky Security Center Linux. Перенос данных с использованием резервной копии данных Сервера администрирования поддерживается только для переноса в Kaspersky Security Center Linux 15.2 или более позднюю версию из любой поддерживаемой версии Kaspersky Security Center Windows.

Если вы используете MySQL или MariaDB в качестве СУБД для Kaspersky Security Center Windows и для Kaspersky Security Center Linux, параметр `lower_case_table_names` должен совпадать в текущей и новой СУБД. Иначе данные Сервера администрирования будут перенесены некорректно.

Прежде чем вы создадите резервную копию данных Сервера администрирования Kaspersky Security Center Windows, проверьте значение параметра `lower_case_table_names`. Если вы не указали этот параметр ранее во время установки СУБД, используется значение параметра по умолчанию. Значение параметра `lower_case_table_names` по умолчанию для Windows – `1`.

При установке MySQL или MariaDB для Kaspersky Security Center Linux установите то же значение параметра `lower_case_table_names`, которое указано для этого параметра для Windows. Подробнее см. инструкцию с веб-сайта MySQL. Если вы не указали этот параметр, используется значение параметра по умолчанию. Для операционных систем на основе Linux значение параметра `lower_case_table_names` по умолчанию отличается от значения по умолчанию для Windows.

Если вы хотите установить MySQL 8.0, параметр `lower_case_table_names`, который задан в соответствии с этой инструкцией может, не сработать. В этом случае сначала вам нужно установить MySQL 5.7, указать параметр `lower_case_table_names`, как описано в инструкции, а затем обновить MySQL 5.7 до MySQL 8.0. Если параметр `lower_case_table_names` не совпадает в текущей и новой СУБД, данные Сервера администрирования будут восстановлены некорректно.

Оптимизация процесса копирования и восстановления данных Сервера администрирования

Для оптимизации резервного копирования и восстановления данных Сервера администрирования с целью сокращения времени простоя Сервера администрирования выполните одно из следующих действий:

- Включите параметр **Использовать моментальный снимок файловой системы для резервного копирования данных**.

  Подробную информацию см. в разделе Использование снимка файловой системы для уменьшения времени резервного копирования.

- Настройте следующие флаги:

Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

- `KLSRV_BKP_FILES` – разбивает файл базы данных на несколько файлов (от 2 до 32) меньшего размера. Это может ускорить резервное копирование и восстановление, если производительность СУБД ограничена процессором.

  Пример:

  ```
  klscflag -fset -pv klserver -n KLSRV_BKP_FILES -t d -v 2
  ```

- `KLSRV_BKP_BACKUP_EXTRA_PARS` – определяет параметры `COMPRESSION` и `MAXTRANSFERSIZE`. Это может ускорить резервное копирование, если производительность СУБД ограничена файловым вводом/выводом.

  Пример:

  ```
  klscflag -fset -pv klserver -n KLSRV_BKP_BACKUP_EXTRA_PARS -t s -v "COMPRESSION,
  MAXTRANSFERSIZE = 4194304"
  ```

- `KLSRV_BKP_RESTORE_EXTRA_PARS` – определяет параметр `MAXTRANSFERSIZE`. Это может ускорить восстановление, если производительность СУБД ограничена файловым вводом/выводом.

  Пример:

  ```
  klscflag -fset -pv klserver -n KLSRV_BKP_RESTORE_EXTRA_PARS -t s -v "MAXTRANSFERSIZE
  = 4194304"
  ```

- `KLSRV_BKP_ONLINE_DB_BACKUP` – устраняет простой Сервера администрирования во время резервного копирования. Доступно только для следующих СУБД:

  - PostgreSQL, Postgres Pro.
  - SQL Server с моделью полного восстановления. Дополнительную информацию см. в документации SQL Server. При включении флага `KLSRV_BKP_ONLINE_DB_BACKUP` СУБД SQL Server автоматически переключается на модель полного восстановления.

  Пример:

  ```
  klscflag.exe -fset -pv klserver -n KLSRV_BKP_ONLINE_DB_BACKUP -t d -v 1
  ```

Перенос Сервера администрирования на другое устройство

Если вам нужно использовать Сервер администрирования на новом устройстве, вы можете перенести его одним из следующих способов:

- Переместить Сервер администрирования и сервер базы данных на новое устройство (сервер базы данных может быть установлен на новом устройстве вместе с Сервером администрирования или на другом устройстве).
- Оставить сервер баз данных на старом устройстве и перенести на новое устройство только Сервер администрирования.

Чтобы перенести Сервер администрирования на новое устройство:

1. На предыдущем устройстве создайте резервную копию данных Сервера администрирования.

Для этого запустите задачу резервного копирования данных с помощью Консоли администрирования или запустите утилиту klbackup.

Если вы используете SQL Server в качестве СУБД для Сервера администрирования, можно перенести данные с SQL Server на СУБД MySQL или MariaDB. Для создания резервной копии данных запустите утилиту klbackup в интерактивном режиме. В окне **Параметры резервного копирования** мастера резервного копирования и восстановления данных включите параметр **Перенос данных в формате MySQL/MariaDB**. Kaspersky Security Center создаст резервную копию, совместимую с MySQL и MariaDB. После этого вы можете восстановить данные из резервной копии в MySQL или MariaDB.

Также можно включить параметр **Перенести в формат Azure**, если вы хотите перенести данные из SQL Server в СУБД Azure SQL.

2. На предыдущем устройстве отключите Сервер администрирования от сети.

3. Выберите новое устройство, на которое будет установлен Сервер администрирования. Убедитесь, что аппаратное и программное обеспечение на выбранном устройстве соответствует требованиям для Сервера администрирования, Консоли администрирования и Агента администрирования. Проверьте, что порты, используемые на Сервере администрирования доступны.

4. Назначьте новому устройству тот же адрес.

   Новому Серверу администрирования можно присвоить имя NetBIOS, FQDN и статический IP-адрес. Это зависит от того, какой адрес Сервера администрирования был установлен в инсталляционном пакете Агента администрирования, когда были развернуты Агенты администрирования. Также вы можете использовать адрес подключения, определяющий Сервер администрирования, к которому подключается Агент администрирования (вы можете получить этот адрес на управляемых устройствах с помощью утилиты klnagchk).

5. При необходимости на другом устройстве установите систему управления базами данных (СУБД), которую будет использовать Сервер администрирования.

   База данных может быть установлена на новом устройстве вместе с Сервером администрирования или на другом устройстве. Убедитесь, что это устройство соответствует аппаратным и программным требованиям. При выборе СУБД учитывайте количество устройств, которые обслуживает Сервер администрирования.

6. Запустите установку Сервера администрирования на новом устройстве.

7. Во время установки Сервера администрирования настройте параметры подключения к серверу баз данных.



Пример окна параметров подключения для Microsoft SQL Server

В зависимости от того, где вам нужно разместить сервер базы данных, выполните одно из следующих действий:

- **Оставьте сервер базы данных на предыдущем устройстве.**

  1. Нажмите на кнопку **Обзор** рядом с полем **Имя экземпляра SQL-сервера** и выберите имя предыдущего устройства в появившемся списке.

     Обратите внимание, что предыдущее устройство должно быть доступно для связи с новым Сервером администрирования.

  2. Введите имя предыдущей базы данных в поле **Имя базы данных**.

- **Переместите сервер базы данных на другое устройство.**

  1. Нажмите на кнопку **Обзор** рядом с полем **Имя экземпляра SQL-сервера** и выберите имя устройства в появившемся списке.

  2. Введите имя новой базы данных в поле **Имя базы данных**.

     Обратите внимание, что имя новой базы данных должно совпадать с именем базы данных на предыдущем устройстве. Имена баз должны совпадать, чтобы можно было использовать резервную копию Сервера администрирования. Имя базы данных по умолчанию *KAV*.

8. После завершения установки восстановите данные Сервера администрирования на новом устройстве с помощью утилиты klbackup.

> Если вы используете SQL Server в качестве СУБД на предыдущем и новом устройствах, обратите внимание, что версия SQL Server, установленная на новом устройстве, должна быть такой же или выше, чем версия SQL Server, установленная на предыдущем устройстве. Иначе вы не сможете восстановить данные Сервера администрирования на новом устройстве.

9. Откройте Консоль администрирования и подключитесь к Серверу администрирования.

10. Убедитесь, что все управляемые устройства подключены к Серверу администрирования.

11. Удалите Сервер администрирования и сервер баз данных с предыдущего устройства.

Также можно использовать Kaspersky Security Center Web Console, чтобы перенести Сервер администрирования и сервер баз данных на другое устройство.

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:

- Поиск устройств.
- Выборки устройств.
- Правила перемещения устройств.
- Правила автоматического назначения тегов.

Чтобы сбросить атрибут Под управлением другого Сервера администрирования:

1. В главном меню Kaspersky Security Center Web Console перейдите в раздел **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.

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 права **Изменение** в области **Управление группами администрирования**, для групп, которыми вы хотите управлять (или для Сервера администрирования, к которому относятся эти группы).

Создание групп администрирования

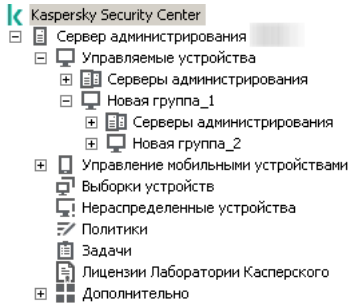
Иерархия групп администрирования формируется в главном окне приложения Kaspersky Security Center в папке **Управляемые устройства**. Группы администрирования отображаются в виде папок в дереве консоли (см. рис. ниже).

Сразу после установки Kaspersky Security Center папка **Управляемые устройства** содержит только пустую папку **Серверы администрирования**.

> Наличие или отсутствие папки **Серверы администрирования** в дереве консоли определяется параметрами пользовательского интерфейса. Для включения отображения этой папки нужно перейти в меню **Вид** → **Настройка интерфейса** и в открывшемся окне **Настройка интерфейса** установить флажок **Отображать подчиненные Серверы администрирования**.

При создании иерархии групп администрирования в состав папки **Управляемые устройства** можно включать устройства и виртуальные машины и добавлять вложенные группы. В папку **Серверы администрирования** можно добавлять подчиненные и виртуальные Серверы администрирования.

Каждая созданная группа, как и папка **Управляемые устройства**, сначала содержит только пустую папку **Серверы администрирования** для работы с подчиненными и виртуальными Серверами администрирования этой группы. Информация о политиках и задачах этой группы, а также информация об устройствах, входящих в эту группу, отображается на вкладках с соответствующими именами в рабочей области этой группы.



Просмотр иерархии групп администрирования

Вы можете сформировать структуру групп администрирования автоматически или создать группы администрирования вручную.

Чтобы создать группу администрирования:

1. В дереве консоли откройте папку **Управляемые устройства**.
2. Если вы хотите создать подгруппу существующей группы администрирования, в папке **Управляемые устройства** выберите вложенную папку, соответствующую группе, в состав которой должна входить новая группа администрирования.

   Если вы создаете новую группу администрирования верхнего уровня иерархии, этот шаг можно пропустить.
3. Запустите процесс создания группы администрирования одним из следующих способов:
   - с помощью команды контекстного меню **Создать → Группу**;
   - по кнопке **Новая группа**, расположенной в рабочей области главного окна приложения на вкладке **Устройства**.
4. В открывшемся окне **Имя группы** введите имя группы и нажмите на кнопку **ОК**.

В результате в дереве консоли появится новая папка группы администрирования с заданным именем.

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 дереве консоли выберите папку **Управляемые устройства**.
2. В контекстном меню папки **Управляемые устройства** выберите пункт **Все задачи → Новая структура групп**.

В результате запускается мастер создания структуры групп администрирования. Следуйте далее указаниям мастера.

Перемещение групп администрирования

Вы можете перемещать вложенные группы администрирования внутри иерархии групп.

Группа администрирования перемещается вместе со всеми вложенными группами, подчиненными Серверами администрирования, устройствами, групповыми политиками и задачами. К ней будут применены все параметры, соответствующие ее новому положению в иерархии групп администрирования.

Имя группы должно быть уникальным в пределах одного уровня иерархии. Если в папке, в которую вы перемещаете группу администрирования, уже существует группа с аналогичным названием, перед перемещением название группы следует изменить. Если вы предварительно не изменили название перемещаемой группы, к ее названию при перемещении автоматически добавляется окончание вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Невозможно изменить название группы **Управляемые устройства**, поскольку она является встроенным элементом Консоли администрирования.

Чтобы переместить группу в другую папку дерева консоли:

1. Выберите перемещаемую группу в дереве консоли.
2. Выполните одно из следующих действий:
   - Переместите группу с помощью контекстного меню:
     1. В контекстном меню группы выберите пункт **Вырезать**;
     2. В контекстном меню группы администрирования, в которую нужно переместить выбранную группу, выберите пункт **Вставить**.
   - Переместите группу с помощью главного меню приложения:
     a. Выберите пункт главного меню **Действие** → **Вырезать**.
     b. Выберите в дереве консоли группу администрирования, в которую нужно переместить выбранную группу.
     c. Выберите пункт главного меню **Действие** → **Вставить**.
   - Переместите группу в другую группу в дереве консоли с помощью мыши.

Удаление групп администрирования

Вы можете удалить группу администрирования, если она не содержит подчиненных Серверов администрирования, вложенных групп и клиентских устройств и если для нее не сформированы задачи и политики.

Перед удалением группы администрирования требуется удалить из ее состава подчиненные Серверы администрирования, вложенные группы и клиентские устройства.

Чтобы удалить группу:

1. В дереве консоли выберите группу администрирования.
2. Выполните одно из следующих действий:
   - в контекстном меню группы выберите пункт **Удалить**;
   - в главном меню приложения выберите пункт **Действие** → **Удалить**;
   - нажмите на кнопку **DELETE**.

Автоматическое создание структуры групп администрирования

Kaspersky Security Center позволяет автоматически сформировать структуру групп администрирования с помощью мастера создания структуры групп.

Мастер создает структуру групп администрирования на основе следующих данных:

- структуры доменов и рабочих групп сети Windows;
- структуры групп Active Directory;
- содержимого текстового файла, созданного администратором вручную.

При формировании текстового файла требуется соблюдать следующие правила:

- Имя каждой новой группы должно начинаться с новой строки; разделитель должен начинаться с разрыва строки. Пустые строки игнорируются.

  Пример:

  Офис 1

  Офис 2

  Офис 3

  В группе назначения будут созданы три группы первого уровня иерархии.

- Имя вложенной группы следует указывать через косую черту (/).

  Пример:

  Офис 1/Подразделение 1/Отдел 1/Группа 1

  В группе назначения будут созданы четыре вложенные друг в друга подгруппы.

- Чтобы создать несколько вложенных групп одного уровня иерархии, следует указать "полный путь к группе".

  Пример:

  Офис 1/Подразделение 1/Отдел 1

  Офис 1/Подразделение 2/Отдел 1

  Офис 1/Подразделение 3/Отдел 1

  Офис 1/Подразделение 4/Отдел 1

  В группе назначения будет создана одна группа первого уровня иерархии "Офис 1", в состав которой будут входить четыре вложенные группы одного уровня иерархии: "Подразделение 1", "Подразделение 2", "Подразделение 3" и "Подразделение 4". В состав каждой из этих групп будет входить группа "Отдел 1".

Создание структуры групп администрирования с помощью мастера не нарушает целостности сети: новые группы добавляются, а не замещают существующие. Клиентское устройство не может быть включено в состав группы администрирования повторно, поскольку при перемещении устройства в группу администрирования оно удаляется из группы **Нераспределенные устройства**.

Если при создании структуры групп администрирования устройство по каким-либо причинам не было включено в состав группы **Нераспределенные устройства** (было выключено, отключено от сети), оно не будет автоматически перенесено в группу администрирования. Вы можете добавить устройства в группы администрирования вручную после завершения работы мастера.

Чтобы запустить автоматическое создание структуры групп администрирования:

1. Выберите в дереве консоли папку **Управляемые устройства**.
2. В контекстном меню папки **Управляемые устройства** выберите пункт **Все задачи** → **Новая структура групп**.

   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. Выберите в дереве консоли нужную вам группу администрирования.
2. Откройте окно свойств этой группы администрирования.
3. В панели **Разделы** выберите **Автоматическая установка**, а затем в рабочей области выберите инсталляционные пакеты приложений, которые следует устанавливать на устройства.
4. Нажмите на кнопку **ОК**.

Групповые задачи созданы. Эти задачи будут запускаться на клиентских устройствах сразу после их добавления в группу администрирования.

Если для автоматической установки указано несколько инсталляционных пакетов одного приложения, задача установки будет создана только для последней версии приложения.

Управление клиентскими устройствами

Этот раздел содержит информацию о работе с клиентскими устройствами.

Подключение клиентских устройств к Серверу администрирования

Подключение клиентского устройства к Серверу администрирования осуществляет Агент администрирования, установленный на клиентском устройстве.

При подключении клиентского устройства к Серверу администрирования выполняются следующие операции:

- Автоматическая синхронизация данных:
  - синхронизация списка приложений, установленных на клиентском устройстве;
  - синхронизация политик, параметров приложений, задач и параметров задач.
- Получение Сервером текущей информации о состоянии приложений, выполнении задач и статистики работы приложений.
- Доставка на Сервер информации о событиях, которые требуется обработать.

Автоматическая синхронизация данных производится периодически, в соответствии с параметрами Агента администрирования (например, один раз в 15 минут). Вы можете вручную задать интервал между соединениями.

Информация о событии доставляется на Сервер администрирования сразу после того, как событие произошло.

Если Сервер администрирования является удаленным, то есть находится вне сети организации, клиентские устройства подключаются к нему через интернет.

Для подключения устройств к Серверу администрирования через интернет должны быть выполнены следующие условия:

- Удаленный Сервер администрирования должен иметь внешний IP-адрес, и на нем должен быть открыт входящий порт 13000 (для подключения от Агентов администрирования). Рекомендуется также открыть порт UDP 13000 (для приема уведомлений о выключении устройств).
- На устройствах должны быть установлены Агенты администрирования.
- При установке Агента администрирования на устройства должен быть указан внешний IP-адрес удаленного Сервера администрирования. Если для установки используется инсталляционный пакет, внешний IP-адрес требуется указать вручную в свойствах инсталляционного пакета в разделе **Параметры**.
- Для управления приложениями и задачами устройства с помощью удаленного Сервера администрирования требуется установить флажок **Не разрывать соединение с Сервером администрирования** в окне свойств этого устройства в разделе **Общие**. После установки флажка необходимо дождаться синхронизации Сервера администрирования с удаленным устройством. Непрерывное соединение с Сервером администрирования могут поддерживать не более 300 клиентских устройств одновременно.

Для ускорения выполнения задач, поступающих от удаленного Сервера администрирования, можно открыть на устройстве порт 15000. В этом случае для запуска задачи Сервер администрирования посылает специальный пакет Агенту администрирования по порту 15000, не дожидаясь синхронизации с устройством.

Kaspersky Security Center позволяет настроить соединение клиентского устройства с Сервером администрирования таким образом, чтобы соединение не завершалось по окончании выполнения операций. Непрерывное соединение необходимо в том случае, если требуется постоянный контроль состояния приложений, а Сервер администрирования не может инициировать соединение с клиентским устройством (например, соединение защищено сетевым экраном, запрещено открывать порты на клиентском устройстве, неизвестен IP-адрес клиентского устройства). Установить неразрывное соединение клиентского устройства с Сервером администрирования можно в окне свойств устройства, в разделе **Общие**.

Рекомендуется устанавливать непрерывное соединение с наиболее важными устройствами. Общее количество соединений, поддерживаемых Сервером администрирования одновременно, ограничено (до 300).

При синхронизации вручную используется вспомогательный способ подключения, при котором соединение инициирует Сервер администрирования. Перед подключением на клиентском устройстве требуется открыть UDP-порт. Сервер администрирования посылает на UDP-порт клиентского устройства запрос на соединение. В ответ на него производится проверка сертификата Сервера администрирования. Если сертификат Сервера совпадает с копией сертификата на клиентском устройстве, соединение осуществляется.

Запуск процесса синхронизации вручную используется также для получения текущей информации о состоянии приложений, выполнении задач и статистике работы приложений.

Подключение клиентского устройства к Серверу администрирования вручную. Утилита klmover

Если вам требуется подключить клиентское устройство к Серверу администрирования вручную, вы можете воспользоваться утилитой klmover на клиентском устройстве.

При установке на клиентское устройство Агента администрирования утилита автоматически копируется в папку установки Агента администрирования.

Чтобы подключить клиентское устройство к Серверу администрирования вручную с помощью утилиты klmover,

на устройстве запустите утилиту klmover из командной строки.

При запуске из командной строки утилита klmover в зависимости от используемых ключей выполняет следующие действия:

- подключает Агент администрирования к Серверу администрирования с указанными параметрами;
- записывает результаты выполнения операции в файл журнала событий или выводит их на экран.

Вы не можете использовать утилиту klmover для клиентских устройств, подключенных к Серверу администрирования через шлюзы соединения. Для таких устройств необходимо перенастроить Агент администрирования или переустановить Агент администрирования, указав шлюз соединения.

Синтаксис командной строки утилиты:

```
klmover [-logfile <имя файла>] [-address <адрес сервера>] [-pn <номер порта>] [-ps <номер SSL-порта>] [-nossl] [-cert <путь к файлу сертификата>] [-silent] [-dupfix] [-virtserv] [-cloningmode]
```

Для запуска утилиты требуются права администратора.

Описания ключей:

- `-logfile <имя файла>` – записать результаты выполнения утилиты в файл журнала.

  По умолчанию информация сохраняется в стандартном потоке вывода (stdout). Если ключ не используется, результаты и сообщения об ошибках выводятся на экран.

- `-address <адрес сервера>` – адрес Сервера администрирования для подключения.

  В качестве адреса можно указать IP-адрес, NetBIOS- или DNS-имя устройства.

- `-pn <номер порта>` – номер порта, по которому будет осуществляться незашифрованное подключение к Серверу администрирования.

  По умолчанию установлен порт 14000.

- `-ps <номер SSL-порта>` – номер SSL-порта, по которому осуществляется зашифрованное подключение к Серверу администрирования с использованием протокола SSL.

  По умолчанию установлен порт 13000.

- `-nossl` – использовать незашифрованное подключение к Серверу администрирования.

  Если ключ не используется, подключение Агента администрирования к Серверу осуществляется по защищенному SSL-протоколу.

- `-cert <путь к файлу сертификата>` – использовать указанный файл сертификата для аутентификации доступа к Серверу администрирования.

  Если ключ не используется, Агент администрирования получает сертификат при первом подключении к Серверу администрирования.

- `-silent` – запустить утилиту на выполнение в тихом режиме.

  Использование ключа может быть полезно, например, при запуске утилиты из сценария входа при регистрации пользователя.

- `-dupfix` – ключ используется в случае, если установка Агента администрирования была выполнена не традиционным способом, с использованием дистрибутива, а, например, путем восстановления из образа диска.

- `-virtserv` – имя виртуального Сервера администрирования.

- `-cloningmode` – режим клонирования диска Агента администрирования.

  Используйте один из следующих параметров для настройки режима клонирования диска:

  - `-cloningmode` – запрос состояния режима клонирования диска.
  - `-cloningmode 1` – включить режим клонирования диска.
  - `-cloningmode 0` – выключить режим клонирования диска.

- `-nauninstpwd <пароль>` – ключ используется, чтобы указать пароль деинсталляции Агента администрирования.

  Ключ является необязательным.

Например, чтобы подключить Агент администрирования к Серверу администрирования, выполните следующую команду:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

Туннелирование соединения клиентского устройства с Сервером администрирования

Kaspersky Security Center 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.

В частности, туннелирование используется для подключения к удаленному рабочему столу: как для подключения к существующему сеансу, так и для создания нового удаленного сеанса.

Также туннелирование может быть использовано при помощи механизма внешних инструментов. В частности, администратор может запускать таким образом утилиту putty, VNC-клиент и прочие инструменты.

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.

Чтобы произвести туннелирование соединения клиентского устройства с Сервером администрирования:

1. В дереве консоли выберите папку группы, в которую входит клиентское устройство.
2. На вкладке **Устройства** выберите устройство.
3. В контекстном меню устройства выберите пункт **Все задачи → Туннелирование соединения**.
4. Создайте туннель в открывшемся окне **Туннелирование соединения**.

Удаленное подключение к рабочему столу клиентского устройства

Администратор может 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 администратор получает полный доступ к информации на этом устройстве и может управлять приложениями, установленными на нем.

В этом разделе описывается, как установить соединение с клиентским устройством с операционной системой Windows и клиентским устройством с операционной системой macOS через Агент администрирования.

Подключение к клиентским устройствам с операционной системой Windows

Удаленное подключение к клиентскому устройству с операционной системой Windows можно осуществить двумя способами:

- С помощью стандартного компонента 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.

- С помощью технологии совместного доступа к рабочему столу Windows.

Подключение к клиентскому устройству с операционной системой Windows с помощью подключения к удаленному рабочему столу

Подключение к существующему сеансу удаленного рабочего стола пользователя осуществляется без уведомления пользователя. После подключения администратора к сеансу пользователь устройства будет отключен от сеанса без предварительного уведомления.

Чтобы подключиться к рабочему столу клиентского устройства с помощью компонента "Подключение к удаленному рабочему столу":

1. В дереве консоли администрирования выберите устройство, к которому требуется получить доступ.
2. В контекстном меню устройства выберите пункт **Все задачи → Подключиться к устройству → Новая сессия RDP**.

   В результате будет запущена штатная утилита Windows mstsc.exe для подключения к удаленному рабочему столу.
3. Следуйте указаниям в открывающихся окнах утилиты.

После подключения к клиентскому устройству рабочий стол клиентского устройства доступен в окне удаленного подключения Microsoft Windows.

Подключение к клиентскому устройству с операционной системой Windows с помощью совместного доступа к рабочему столу Windows

При подключении к существующему сеансу удаленного рабочего стола пользователь этого сеанса на устройстве получит запрос от администратора на подключение. Информация о процессе удаленной работы с устройством и результатах этой работы не сохраняется в отчетах Kaspersky Security Center.

Администратор может подключиться к существующему сеансу на клиентском устройстве без отключения пользователя, работающего в этом сеансе. В этом случае у администратора и пользователя сеанса на устройстве есть совместный доступ к рабочему столу.

Администратор может настроить аудит действий на удаленном клиентском устройстве. В ходе аудита приложение сохраняет информацию о файлах на клиентском устройстве, которые открывал и/или изменял администратор.

Для подключения к рабочему столу клиентского устройства с помощью совместного доступа к рабочему столу Windows требуется выполнение следующих условий:

- На рабочем месте администратора установлена операционная система Microsoft Windows Vista или более поздняя версия. Тип операционной системы устройства, на котором установлен Сервер администрирования, не является ограничением для подключения с помощью совместного доступа к рабочему столу Windows.

  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 реестре Windows.
- На клиентском устройстве установлена операционная система Microsoft Windows Vista или более поздняя версия.
- Kaspersky Security Center использует лицензию на Системное администрирование.

Чтобы подключиться к рабочему столу клиентского устройства с помощью совместного доступа к рабочему столу Windows:

1. В дереве консоли администрирования выберите устройство, к которому требуется получить доступ.
2. В контекстном меню устройства выберите пункт **Все задачи → Подключиться к устройству → Совместный доступ к рабочему столу Windows**.
3. В открывшемся окне **Выбор сессии рабочего стола** выберите сеанс на клиентском устройстве, к которому требуется подключиться.

   В случае успешного подключения к клиентскому устройству рабочий стол этого устройства будет доступен в окне **Kaspersky Remote Desktop Session Viewer**.
4. Для начала взаимодействия с устройством в главном меню окна **Kaspersky Remote Desktop Session Viewer** выберите пункт **Действия → Интерактивный режим**.

Для работы утилиты **Kaspersky Remote Desktop Session Viewer** требуется коммерческая лицензия.

Подключение к клиентским устройствам с операционной системой macOS

Администратор может использовать систему Virtual Network Computing (VNC) для подключения к устройствам с операционной системой macOS.

Подключение к удаленному рабочему столу осуществляется с помощью VNC-клиента, установленного на устройстве Сервера администрирования. VNC-клиент переключает управление клавиатурой и мышью с клиентского устройства на администратора.

Когда администратор подключается к удаленному рабочему столу, пользователь не получает уведомлений или запросов на подключение от администратора. Администратор подключается к существующему сеансу на клиентском устройстве без отключения пользователя, работающего в этом сеансе.

Для подключения к рабочему столу клиентского устройства с операционной системой macOS с помощью VNC-клиента требуется выполнение следующих условий:

- VNC-клиент установлен на устройстве Сервера администрирования.
- На клиентском устройстве разрешены удаленный вход и удаленное управление.
- Пользователь разрешил администратору доступ к клиентскому устройству в параметры **Обмен** в операционной системе macOS.

Чтобы подключиться к рабочему столу клиентского устройства с помощью системы Virtual Network Computing:

1. В дереве консоли администрирования выберите устройство, к которому требуется получить доступ.
2. В контекстном меню устройства выберите пункт **Все задачи → Туннелирование соединения**.
3. В открывшемся окне **Туннелирование соединения** выполните одно из следующих действий:

   a. В разделе **1. Сетевой порт** укажите номер порта устройства, к которому требуется подключиться.

      По умолчанию номер порта – 5900.

b. В разделе **2. Туннелирование** нажмите на кнопку **Создать туннель**.

c. В разделе **3. Сетевые атрибуты** нажмите на кнопку **Копировать**.

4. Откройте VNC-клиент и вставьте скопированные сетевые атрибуты в текстовое поле. Нажмите на клавишу **`Enter`**.

5. В появившемся окне просмотрите параметры сертификата. Если вы согласны использовать сертификат, нажмите на кнопку **Да**.

6. В окне **Аутентификация** укажите учетные данные клиентского устройства и нажмите на кнопку **OK**.

Подключение к устройствам с помощью совместного доступа к рабочему столу Windows

Чтобы подключиться к устройству с помощью совместного доступа к рабочему столу Windows:

1. В дереве консоли на вкладке **Устройства** выберите папку **Управляемые устройства**.

   В рабочей области папки отображается список устройств.

2. В контекстном меню устройства, к которому вы хотите подключиться, выберите пункт **Подключиться к устройству → Совместный доступ к рабочему столу Windows**.

   Откроется окно **Выбор сессии рабочего стола**.

3. В окне **Выбор сессии рабочего стола** выберите сеанс рабочего стола, которое будет использоваться для подключения к устройству.

4. Нажмите на кнопку **OK**.

Будет выполнено подключение к устройству.

Настройка перезагрузки клиентского устройства

В ходе работы, установки или удаления Kaspersky Security Center может потребоваться перезагрузка клиентского устройства. Вы можете настроить параметры перезагрузки только для устройств под управлением Windows.

Чтобы настроить перезагрузку клиентского устройства:

1. В дереве консоли выберите группу администрирования, для которой нужно настроить перезагрузку.

2. В рабочей области группы выберите вкладку **Политики**.

3. В списке политик выберите политику Агента администрирования Kaspersky Security Center и в контекстном меню политики выберите пункт **Свойства**.

4. В окне свойств политики выберите раздел **Управление перезагрузкой**.

5. Выберите действие, которое нужно выполнять, если потребуется перезагрузка устройства:

   - Выберите **Не перезагружать операционную систему**, чтобы запретить автоматическую перезагрузку.
   - Выберите **При необходимости перезагрузить операционную систему автоматически**, чтобы разрешить автоматическую перезагрузку.
   - Выберите **Запрашивать у пользователя**, чтобы включить запрос на перезагрузку у пользователя.

   Вы можете указать периодичность запроса на перезагрузку, включить принудительную перезагрузку и принудительное закрытие приложений в заблокированных сеансах на устройстве, установив соответствующие флажки и интервалы.

6. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно свойств политики.

В результате перезагрузка операционной системы устройства будет настроена.

Аудит действий на удаленном клиентском устройстве

Приложение позволяет выполнять аудит действий администратора на удаленных клиентских устройствах под управлением Windows. В ходе аудита приложение сохраняет информацию о файлах на устройстве, которые открывал и/или изменял администратор. 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.

Чтобы включить аудит действий на удаленном клиентском устройстве:

1. В дереве консоли выберите группу администрирования, для которой нужно настроить аудит действий администратора.
2. В рабочей области группы выберите вкладку **Политики**.
3. Выберите политику Агента администрирования Kaspersky Security Center и в контекстном меню политики выберите пункт **Свойства**.
4. В окне свойств политики выберите раздел **Совместный доступ к рабочему столу Windows**.
5. Установите флажок **Включить аудит**.
6. В списки **Маски файлов, чтение которых нужно отслеживать** и **Маски файлов, изменение которых нужно отслеживать** добавьте маски файлов, для которых приложение будет контролировать действия во время аудита.

   По умолчанию приложение отслеживает действия с файлами с расширениями .txt, .rtf, .doc, .xls, .docx, .xlsx, .odt, and .pdf.

7. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно свойств политики.

В результате аудит действий администратора на удаленном устройстве пользователя при использовании общего доступа к рабочему столу будет настроен.

Записи о действиях администратора на удаленном устройстве сохраняются:

- в журнале событий на удаленном устройстве;
- в файле с расширением syslog, который находится в папке Агента администрирования на удаленном устройстве (например, C:\ProgramData\KasperskyLab\adminkit\1103\logs);
- в базе событий Kaspersky Security Center.

Проверка соединения клиентского устройства с Сервером администрирования

Kaspersky Security Center позволяет проверять соединение клиентского устройства с Сервером администрирования автоматически или вручную.

Автоматическая проверка соединения осуществляется на Сервере администрирования. Проверка соединения вручную осуществляется на устройстве.

Автоматическая проверка соединения клиентского устройства с Сервером администрирования

Чтобы запустить автоматическую проверку соединения клиентского устройства с Сервером администрирования:

1. В дереве консоли выберите группу администрирования, в которую входит устройство.
2. В рабочей области группы администрирования на вкладке **Устройства** выберите устройство.
3. В контекстном меню устройства выберите пункт **Проверить доступность устройства**.

В результате открывается окно, содержащее информацию о доступности устройства.

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 FAQ.

О проверке времени соединения устройства с Сервером администрирования

При выключении устройства Агент администрирования уведомляет Сервер администрирования о выключении. В Консоли администрирования такое устройство отображается как выключенное. Однако Агенту удается уведомить Сервер администрирования не во всех случаях. Поэтому Сервер администрирования для каждого устройства периодически анализирует атрибут **Соединение с Сервером администрирования** (значение атрибута отображается в Консоли администрирования в свойствах устройства в разделе **Общие**) и сопоставляет его с периодом синхронизации из действующих параметров Агента администрирования. Если устройство не выходило на связь более чем три периода синхронизации, то такое устройство отмечается как выключенное.

Идентификация клиентских устройств на Сервере администрирования

Идентификация клиентских устройств осуществляется на основании их имен. Имя устройства является уникальным среди всех имен устройств, подключенных к Серверу администрирования.

Имя устройства передается на Сервер администрирования либо при опросе сети Windows и обнаружении в ней нового устройства, либо при первом подключении к Серверу администрирования установленного на устройство Агента администрирования. По умолчанию имя совпадает с именем устройства в сети Windows (NetBIOS-имя). Если на Сервере администрирования уже зарегистрировано устройство с таким именем, то к имени нового устройства будет добавлено окончание с порядковым номером, например: **<Имя>-1**, **<Имя>-2**. Под этим именем устройство включается в состав группы администрирования.

Перемещение устройств в состав группы администрирования

Устройства можно перемещать из одной группы администрирования в другую только при наличии прав **Изменение** в области **Управление группами администрирования** как для исходных, так и для целевых групп администрирования (или для Сервера администрирования, к которым принадлежат эти группы).

Чтобы включить одно или несколько устройств в состав выбранной группы администрирования:

1. В дереве консоли откройте папку **Управляемые устройства**.
2. В папке **Управляемые устройства** выберите вложенную папку, соответствующую группе, в состав которой будут включены клиентские устройства.

   Если вы хотите включить устройства в состав группы **Управляемые устройства**, этот шаг можно пропустить.
3. В рабочей области выбранной группы администрирования на вкладке **Устройства** запустите процесс включения устройств в группу одним из следующих способов:

   - Добавьте устройства в группу по кнопке **Переместить устройства в группу** в блоке работы со списком устройств.
   - В контекстном меню списка устройств выберите **Создать** → **Устройство**.

   В результате запустится мастер перемещения устройств. Следуя его указаниям, определите способ перемещения устройств в группу и сформируйте список устройств, включаемых в состав группы.

   Если вы формируете список устройств вручную, в качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал), NetBIOS- или DNS-имя. Вручную в список устройств могут быть перемещены только те устройства, информация о которых уже была добавлена в базу данных Сервера администрирования при подключении устройства или в результате обнаружения устройств.

   Для импорта списка устройств из файла требуется указать файл в формате TXT с перечнем адресов добавляемых устройств. Каждый адрес должен располагаться в отдельной строке.

После завершения работы мастера выбранные устройства включаются в состав группы администрирования и отображаются в списке устройств под именами, установленными для них Сервером администрирования.

Можно переместить устройство в выбранную группу администрирования, перетащив его мышью из папки **Нераспределенные устройства** в папку группы администрирования.

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*.

Чтобы сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером:

1. В дереве консоли выберите папку **Задачи**.
2. По кнопке **Новая задача** в рабочей области папки запустите мастер создания задачи.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. На шаге мастера **Выбор типа задачи** выберите узел **Сервер администрирования Kaspersky Security Center**, откройте папку **Дополнительно** и выберите задачу **Смена Сервера администрирования**.
4. В открывшемся окне нажмите на кнопку **ОК**, чтобы подтвердить свое согласие с условиями смены Сервера администрирования для клиентских устройств.
5. На шаге мастера **Параметры** выберите Сервер администрирования, который вы хотите использовать для управления выбранными устройствами:

   - **Подключение к главному Серверу администрирования**

     Чтобы переместить клиентские устройства на другой главный Сервер администрирования, укажите следующие параметры подключения к Серверу администрирования:

     1. В поле **Сервер администрирования** укажите адрес нового главного Сервера администрирования.
     2. В поле **Порт** укажите номер порта для подключения к Серверу администрирования.

        По умолчанию установлен порт 14000.
     3. В поле **SSL-порт** укажите номер SSL-порта главного Сервера администрирования.

        По умолчанию установлен порт 13000.
     4. При необходимости установите флажок **Использовать прокси-сервер**.

        Если этот флажок снят, для подключения устройства к Серверу администрирования используется прямое соединение.

        Если этот флажок установлен, укажите параметры прокси-сервера:

        - **Адрес прокси-сервера**
        - **Порт прокси-сервера**

        Если ваш прокси-сервер требует аутентификации, в полях **Имя пользователя** и **Пароль** укажите учетные данные учетной записи, под которой устанавливается соединение с прокси-сервером. Рекомендуется указывать данные учетной записи с минимальными правами, необходимыми только для аутентификации на прокси-сервере.
     5. При необходимости загрузите новый сертификат Сервера администрирования.

   - **Добавление подчиненного Сервера на главный Сервер**

     Выберите этот параметр, чтобы переместить на виртуальный Сервер администрирования клиентские устройства на текущем главном Сервере администрирования. Для этого в поле **Имя виртуального Сервера администрирования** укажите имя нужного виртуального Сервера администрирования.

При необходимости укажите время ожидания перед перезапуском Агента администрирования.

6. На этом шаге мастера выберите устройства, которым будет назначена задача:

   - **Выбрать устройства, обнаруженные в сети Сервером администрирования**. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

   - **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.

   - **Назначить задачу выборке устройств**. В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать предопределенную выборку или вашу собственную выборку.

   - **Назначить задачу группе администрирования**. В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.

7. На шаге мастера **Выбор учетной записи для запуска задачи** укажите параметры учетной записи:

   - **Учетная запись по умолчанию**

     Задача будет запускаться под той же учетной записью, под которой было установлено и запущено приложение, выполняющее эту задачу.

     По умолчанию выбран этот вариант.

   - **Задать учетную запись**

     В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.

     - **Учетная запись**

       Учетная запись, от имени которой будет запускаться задача.

     - **Пароль**

       Пароль учетной записи, от имени которой будет запускаться задача.

8. На шаге **Настройка расписания запуска задачи** мастера можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

   - **Запуск по расписанию:**

     Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

     - **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.

       По умолчанию задача запускается каждый день в текущее системное 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.

- **Один раз**

  Задача выполняется один раз, в указанные дату и время (по умолчанию в день создания задачи).

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

  По умолчанию выбран этот вариант.

- **Немедленно**

  Задача запускается сразу после того, как устройство становится видимым в сети или сразу после включения устройства в область действия задачи.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию. Для расписания **Вручную**, **Один раз** и **Немедленно** задачи выполняются только на тех клиентских устройствах, которые видны в сети. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр выключен.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

9. На этом шаге мастера укажите имя создаваемой задачи.

10. На странице **Завершение создания задачи** мастера нажмите на кнопку **Готово**, чтобы завершить работу мастера.

    Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

После завершения работы задачи клиентские устройства, для которых она была создана, переходят под управление Сервера администрирования, указанного в параметрах задачи.

Если Сервер администрирования поддерживает управление шифрованием и защитой данных, то при создании задачи *Смена Сервера администрирования* отображается предупреждение. Предупреждение содержит информацию о том, что при наличии на устройствах зашифрованных данных после переключения устройств под управлением другого Сервера пользователям будет предоставлен доступ только к тем зашифрованным данным, с которыми они работали ранее. В остальных случаях доступ к зашифрованным данным предоставлен не будет. Подробное описание сценариев, в которых доступ к зашифрованным данным не будет предоставлен, приведено в справке Kaspersky Endpoint Security для Windows.

Перемещение устройств, подключенных к Серверу администрирования через шлюзы соединения, на другой Сервер администрирования

Вы можете перемещать устройства, подключенные к Серверу администрирования через шлюзы соединения, на другой Сервер администрирования Например, это может потребоваться, если вы устанавливаете другую версию Сервера администрирования и не хотите переустанавливать Агент администрирования на устройствах, поскольку это может занять много времени.

Команды, описанные в инструкции, нужно выполнить на клиентских устройствах под учетной записью с правами администратора.

Чтобы переместить устройство, подключенное через шлюз соединения, на другой Сервер администрирования:

1. Запустите утилиту klmover с параметром `-address <Server address>`, чтобы переключиться на новый Сервер администрирования.

2. Выполните команду `klnagchk -nagwait -tl 4`.

3. Выполните следующие команды для установки нового шлюза соединения:

   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "<Connection gateway IP address or name>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     Здесь `<Connection gateway IP address or name>` – адрес шлюза соединения, доступного из интернета.

   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `13000` – это номер TCP-порта, который прослушивает шлюз соединения.

4. Выполните команду `klnagchk -restart -tl 4` для запуска службы Агента администрирования.

Устройство будет перемещено на новый Сервер администрирования и подключено через новый шлюз соединения.

Кластеры и массивы серверов

Kaspersky Security Center поддерживает кластерную технологию. Если Агент администрирования передает Серверу администрирования информацию о том, что приложение, установленное на клиентском устройстве, является частью массива сервера, то клиентское устройство становится узлом кластера. Кластер будет добавлен как отдельный объект в папке **Управляемые устройства** в дереве консоли со значками серверов ().

Можно выделить несколько типичных свойств кластера:

- Кластер и любой из его узлов всегда располагаются в одной группе администрирования.
- Если администратор попытается переместить какой-либо узел кластера, то узел вернется в исходное местоположение.
- Если администратор попытается переместить кластер в другую группу, то все его узлы также переместятся вместе с ним.

Удаленное включение, выключение и перезагрузка клиентских устройств

Kaspersky Security Center позволяет удаленно управлять клиентскими устройствами, включать, выключать и перезагружать их.

Чтобы удаленно управлять клиентскими устройствами:

1. Подключитесь к Серверу администрирования, под управлением которого находятся устройства.
2. Создайте задачу управления устройствами одним из следующих способов:
   - Если требуется включить, выключить или перезагрузить устройства, входящие в выбранную группу администрирования, создайте задачу для выбранной группы.
   - Если требуется включить, выключить или перезагрузить устройства, входящие в разные группы администрирования или не входящие в группы администрирования, создайте задачу для набора устройств.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера. В окне **Выбор типа задачи** мастера создания задачи выберите узел **Kaspersky Security Center**, раскройте папку **Дополнительно** и выберите задачу **Управление устройствами**.
3. Запустите созданную задачу.

После завершения работы задачи команда (включение, выключение или перезагрузка) будет выполнена на выбранных устройствах.

Об использовании постоянного соединения между управляемым устройством и Сервером администрирования

По умолчанию в Kaspersky Security Center нет постоянных соединений между управляемыми устройствами и Сервером администрирования. Агенты администрирования на управляемых устройствах периодически устанавливают соединение и синхронизируются с Сервером администрирования. Интервал между этими сеансами синхронизации определяется в политике Агента администрирования и по умолчанию составляет 15 минут. Если необходима досрочная синхронизация (например, для ускорения применения политики), то Сервер администрирования посылает Агенту администрирования подписанный сетевой пакет на порт UDP 15000. Сервер администрирования может отправить этот пакет по IPv4-сети или IPv6-сети. Если подключение по UDP от Сервера администрирования к управляемому устройству по какой-то причине невозможно, то синхронизация произойдет при очередном периодическом подключении Агента администрирования к Серверу в течение периода синхронизации.

Однако некоторые операции невозможно выполнить без подключения Агента администрирования к Серверу администрирования. Эти операции включают запуск и остановку локальных задач, получение статистики для управляемого приложения и создание туннеля. Чтобы эти операции стали возможными, необходимо включить на управляемом устройстве параметр **Не разрывать соединение с Сервером администрирования**.

О принудительной синхронизации

Несмотря на то что Kaspersky Security Center автоматически синхронизирует состояние, параметры, задачи и политики для управляемых устройств, в отдельных случаях администратору нужно точно знать, что в текущий момент для определенного устройства синхронизация выполнена.

В контекстном меню управляемых устройств в Консоли администрирования в пункте меню **Все задачи** имеется команда **Синхронизировать принудительно**. Когда Kaspersky Security Center 15.1 выполняет эту команду, Сервер администрирования пытается подключиться к устройству. Если эта попытка успешна, будет выполнена принудительная синхронизация. В противном случае принудительная синхронизация произойдет только после очередного выхода Агента администрирования на связь с Сервером.

О расписании соединений

В окне свойств политики Агента администрирования в разделе **Подключения** во вложенном 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.

Подключаться в указанные периоды. Если выбран этот вариант, подключение Агента администрирования к Серверу администрирования выполняется в заданные периоды времени. Можно добавить несколько периодов подключения.

Отправка сообщения пользователям устройств

Чтобы отправить сообщение пользователям устройств:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.

2. Создайте задачу отправки сообщения пользователям устройств одним из следующих способов:

   - Если требуется отправить сообщение пользователям устройств, входящих в выбранную группу администрирования, создайте задачу для выбранной группы.

   - Если требуется отправить сообщение пользователям устройств, входящих в разные группы администрирования или не принадлежащих ни одной группе администрирования, создайте задачу для набора устройств.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

3. В окне Тип задачи мастера создания задачи выберите узел **Сервер администрирования Kaspersky Security Center**, раскройте папку **Дополнительно** и выберите задачу **Сообщение для пользователя**. Отправка сообщений пользователю с помощью задачи доступна только для устройств под управлением операционной системы Windows. Также вы можете отправить сообщение из контекстного меню пользователя из рабочей области папки **Управление учетными записями пользователей**.

4. Запустите созданную задачу.

После завершения работы задачи созданное сообщение будет отправлено пользователям выбранных устройств. Отправка сообщений пользователю с помощью задачи доступна только для устройств под управлением операционной системы Windows. Также вы можете отправить сообщение из контекстного меню пользователя из рабочей области папки **Учетные записи пользователей**.

Работа с приложением Kaspersky Security для виртуальных сред

Kaspersky Security Center поддерживает возможность подключения виртуальных машин к Серверу администрирования. Защита виртуальных машин осуществляется с помощью приложения Kaspersky Security для виртуальных сред. Подробнее см. в документации к этому приложению.

Настройка переключения статусов устройств

Вы можете изменить условия присвоения статусов *Критический* или *Предупреждение* устройству.

Чтобы изменить статус устройства на Критический:

1. Откройте окно свойств одним из следующих способов:
   - В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
   - В контекстном меню группы администрирования выберите пункт **Свойства**.
2. В открывшемся окне **Свойства** в панели **Разделы** выберите **Статус устройства**.
3. В разделе **Установить статус 'Критический', если** установите флажок для условия из списка.

   Вы можете изменить только параметры, которые не заблокированы в родительской политике.
4. Откройте окно свойств выбранного условия двойным щелчком мыши по его названию и укажите необходимое значение для условия.

   Вы не можете задать значения для следующих условий: Приложение безопасности не установлено, Установлены несовместимые приложения, Обнаружены уязвимости в приложениях, Параметры мобильного устройства не соответствуют политике, Есть необработанные проблемы безопасности, Статус устройства определен приложением, Устройство стало неуправляемым, Приложение безопасности не запущено, Срок действия лицензии истек.

   Для условия **Требуется перезагрузка** можно указать причины перезагрузки. Рекомендуется установить флажки рядом со всеми причинами из списка.
5. Нажмите на кнопку **OK**.

При выполнении заданных условий управляемому устройству присваивается статус *Критический*.

Чтобы изменить статус устройства на Предупреждение:

1. Откройте окно свойств одним из следующих способов:
   - В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
   - В контекстном меню группы администрирования выберите пункт **Свойства**.
2. В открывшемся окне **Свойства** в панели **Разделы** выберите раздел **Статус устройства**.

3. В разделе **Установить статус 'Предупреждение', если** установите флажок для условия из списка.

   Вы можете изменить только параметры, которые не заблокированы в родительской политике.

4. Откройте окно свойств выбранного условия двойным щелчком мыши по его названию и укажите необходимое значение для условия.

   Вы не можете задать значения для следующих условий: Приложение безопасности не установлено, Установлены несовместимые приложения, Обнаружены уязвимости в приложениях, Параметры мобильного устройства не соответствуют политике, Есть необработанные проблемы безопасности, Статус устройства определен приложением, Устройство стало неуправляемым, Приложение безопасности не запущено, Срок действия лицензии истек.

   Для условия **Требуется перезагрузка** можно указать причины перезагрузки. Рекомендуется установить флажки рядом со всеми причинами из списка.

5. Нажмите на кнопку **ОК**.

При выполнении заданных условий управляемому устройству присваивается статус *Предупреждение*.

Назначение тегов устройствам и просмотр назначенных тегов

Kaspersky Security Center позволяет назначать теги устройствам. *Тег* представляет собой идентификатор устройства, который можно использовать для группировки, описания, поиска устройств. Назначенные устройствам теги можно использовать при создании выборок устройств, при поиске устройств и при распределении устройств по группам администрирования.

Теги могут назначаться устройствам вручную или автоматически. Ручное назначение тегов устройству выполняется в свойствах устройства и может понадобиться, когда необходимо отметить отдельное устройство. Автоматическое назначение тегов выполняется Сервером администрирования в соответствии с заданными правилами назначения тегов.

В свойствах Сервера администрирования вы можете настроить автоматическое назначение тегов устройствам, управляемым этим Сервером администрирования. Автоматическое назначение тегов устройствам происходит при выполнении определенных правил. Каждому тегу соответствует отдельное правило. Правила могут применяться к сетевым свойствам устройства, операционной системе, установленным на устройстве приложениям и другим свойствам устройства. Например, вы можете настроить правило, в соответствии с которым устройствам, работающим под управлением операционной системы Windows, назначается тег *Win*. Затем можно использовать этот тег при создании выборки устройств, чтобы отобрать устройства, работающие под управлением операционной системы Windows, и назначить им задачу.

Вы также можете использовать теги в качестве условия для активации профиля политики на управляемом устройстве, чтобы определенные профили политик применялись только на устройствах, имеющих определенные теги. Например, если в группе администрирования *Пользователи* появляется устройство с тегом *Курьер* и по тегу *Курьер* настроена активация соответствующего профиля политики, то к этому устройству будет применяться не сама политика, созданная для группы *Пользователи*, а ее профиль. Профиль политики может разрешить на этом устройстве запуск отдельных приложений, которые запрещено запускать в рамках политики.

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. Каждое правило назначения тегов можно включить или выключить. Если правило включено, оно применяется к устройствам, управляемым Сервером администрирования. Если правило не нужно, но может понадобиться в дальнейшем, то нет необходимости его удалять; достаточно снять флажок **Включить правило**. При этом правило выключается и не выполняется до тех пор, пока флажок **Включить правило** не будет установлен. Отключение правила без удаления может потребоваться, если это правило необходимо временно исключить из списка правил назначения тегов, а потом опять включить.

Автоматическое назначение тегов устройствам

Вы можете создавать и изменять правила автоматического назначения тегов в окне свойств Сервера администрирования.

Чтобы автоматически назначить теги устройствам:

1. В дереве консоли выберите узел с именем Сервера администрирования, для которого требуется задать правила назначения тегов.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Правила назначения тегов**.
4. В разделе **Правила назначения тегов** нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.
5. В окне **Новое правило** настройте общие свойства правила:

   - Укажите имя правила.

     Имя правила не может превышать 255 символов и содержать специальные символы (`"*<>?\:|`).
   - Включите или выключите правило с помощью флажка **Включить правило**.

     По умолчанию флажок **Включить правило** установлен.
   - В поле **Тег** введите название тега.

     Название тега не может превышать 255 символов и содержать специальные символы (`"*<>?\:|`).
6. В разделе **Условия** нажмите на кнопку **Добавить**, чтобы добавить новое условие, или нажмите на кнопку **Свойства**, чтобы изменить существующее условие.

   Откроется окно мастера создания условия для правила автоматического назначения тегов.
7. В окне **Условие назначения тега** установите флажки для тех условий, которые должны влиять на назначения тега. Можно выбрать несколько условий.

8. В зависимости от того, какие условия назначения тега вы выбрали, мастер покажет окна для настройки соответствующих условий. Настройте срабатывание правила по следующим условиям:

   - **Использование или отношение устройства к определенной сети** – сетевые свойства устройства (например, имя устройства в сети Windows, принадлежность устройства к домену, к IP-диапазону).

     Если для базы данных, которую вы используете для Kaspersky Security Center, настроена сортировка с учетом регистра, учитывайте регистр при указании DNS-имени устройства. Иначе правила автоматического назначения тегов не будет работать.

   - **Использование Active Directory** – нахождение устройства в подразделении Active Directory и членство устройства в группе Active Directory.

   - **Определенные приложения** – наличие на устройстве Агента администрирования, тип, версия и архитектура операционной системы.

   - **Виртуальные машины** – принадлежность устройства к разным типам виртуальных машин.

   - **Установлено приложение из реестра приложений** – наличие на устройстве приложений различных производителей.

9. После настройки условия введите название условия и завершите работу мастера.

   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. Добавленные условия отображаются в окне свойств правила.

10. Нажмите на кнопку **OK** в окне **Новое правило** и на кнопку **OK** в окне свойств Сервера администрирования.

Созданные правила выполняются на устройствах, управляемых выбранным Сервером администрирования. Если параметры устройства соответствуют условиям правила, этому устройству назначается тег.

Просмотр и настройка тегов, назначенных устройству

Вы можете просмотреть список всех тегов, назначенных устройству, а также перейти к настройке правил автоматического назначения тегов в окне свойств устройства.

Чтобы просмотреть и настроить назначенные устройству теги:

1. В дереве консоли откройте папку **Управляемые устройства**.

2. В рабочей области папки **Управляемые устройства** выберите устройство, для которого вы хотите посмотреть назначенные теги.

3. В контекстном меню мобильного устройства выберите пункт **Свойства**.

4. В окне свойств устройства выберите раздел **Теги**.

   Отобразится список тегов, назначенных выбранному устройству, а также способ назначения тега: вручную или по правилу.

5. При необходимости выполните одно из следующих действий:

   - Чтобы перейти к настройке правил назначения тегов, перейдите по ссылке **Настроить правила автоматического назначения тегов** (только для устройств с операционной системой Windows).
   - Чтобы переименовать тег, выделите тег и нажмите на кнопку **Переименовать**.
   - Чтобы удалить тег, выделите тег и нажмите на кнопку **Удалить**.
   - Чтобы добавить тег вручную, введите тег в поле в нижней части раздела **Теги** и нажмите на кнопку **Добавить**.

6. Нажмите на кнопку **Применить**, если вы делали изменения в разделе **Теги**, чтобы ваши изменения вступили в силу.

7. Нажмите на кнопку **OK**.

Если вы удалили или переименовали тег в свойствах устройства, это изменение не распространится на правила назначения тегов, заданные в свойствах Сервера администрирования. Изменение будет применено только к тому устройству, в свойства которого вы внесли изменение.

Удаленная диагностика клиентских устройств. Утилита удаленной диагностики Kaspersky Security Center

Утилита удаленной диагностики Kaspersky Security Center (далее – утилита удаленной диагностики) предназначена для удаленного выполнения на клиентских устройствах следующих операций:

- включения и выключения трассировки, изменения уровня трассировки, загрузки файла трассировки;
- загрузки системной информации и параметров приложения;
- загрузки журналов событий;
- создание файла дампа для приложения;
- запуска диагностики и загрузки результатов диагностики;
- запуска и остановки приложений.

Вы можете использовать журнал событий и диагностические отчеты, загруженные с клиентского устройства, для устранения неполадок самостоятельно. Также специалист Службы 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".

Утилита удаленной диагностики автоматически устанавливается на устройство совместно с Консолью администрирования.

Подключение утилиты удаленной диагностики к клиентскому устройству

Чтобы подключить утилиту удаленной диагностики к клиентскому устройству:

1. В дереве консоли выберите любую группу администрирования.

2. В рабочей области на вкладке **Устройства** в контекстном меню любого устройства выберите пункт **Внешние инструменты → Удаленная диагностика**.

   В результате открывается главное окно утилиты удаленной диагностики.

3. В первом поле главного окна утилиты удаленной диагностики определите, какими средствами требуется подключиться к устройству:

   - **Доступ средствами сети Microsoft Windows**.
   - **Доступ средствами Сервера администрирования**.

4. Если в первом поле главного окна утилиты вы выбрали вариант **Доступ средствами сети Microsoft Windows**:

   - В поле **Устройство** укажите адрес устройства, к которому требуется подключиться.

     В качестве адреса устройства можно использовать IP-адрес, NetBIOS- или DNS-имя.

     По умолчанию указан адрес устройства, из контекстного меню которого запущена утилита.

   - Укажите учетную запись для подключения к устройству:

     - **Подключиться от имени текущего пользователя** (выбрано по умолчанию). Подключитесь под учетной записью текущего пользователя.
     - **При подключении использовать предоставленное имя пользователя и пароль**. Подключитесь под указанной учетной записью. Укажите **Имя пользователя** и **Пароль** нужной учетной записи.

     Подключение к устройству возможно только под учетной записью локального администратора устройства.

5. Если в первом поле главного окна утилиты вы выбрали вариант **Доступ средствами Сервера администрирования**:

   - В поле **Сервер администрирования** укажите адрес Сервера администрирования, с которого следует подключиться к устройству.

     В качестве адреса Сервера можно использовать IP-адрес, NetBIOS- или DNS-имя.

     По умолчанию указан адрес Сервера, с которого запущена утилита.

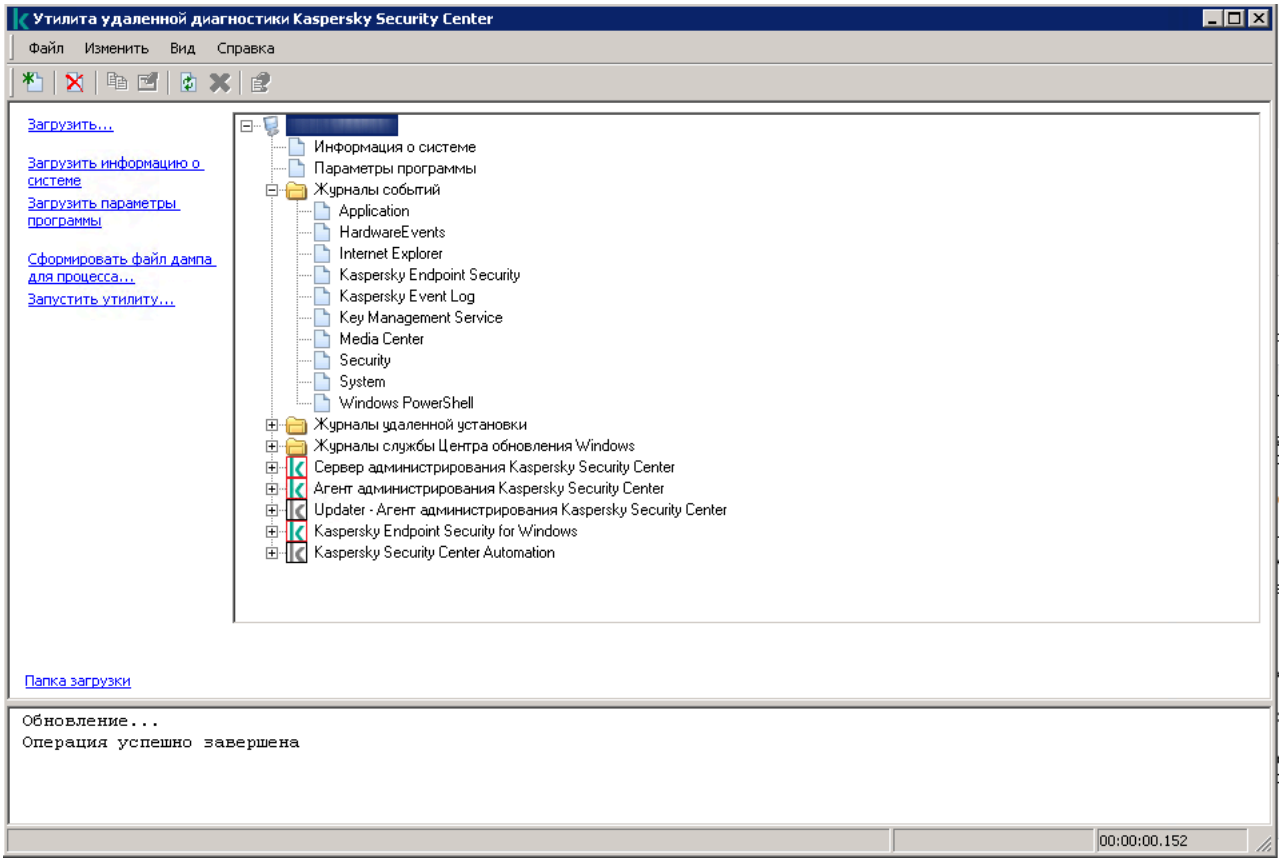
   - Если требуется, установите флажки **Использовать SSL**, **Сжимать трафик** и **Устройство принадлежит подчиненному Серверу администрирования**.

     Если установлен флажок **Устройство принадлежит подчиненному Серверу администрирования**, в поле **Устройство принадлежит подчиненному Серверу администрирования** вы можете выбрать подчиненный Сервер администрирования, под управлением которого находится устройство, нажав на кнопку **Обзор**.

6. Для подключения к устройству нажмите на кнопку **Войти**.

Вам нужно авторизовываться с помощью двухфакторной аутентификации, если двухфакторная аутентификация для вашей учетной записи включена.

В результате откроется окно удаленной диагностики устройства (см. рис. ниже). В левой части окна расположены ссылки для выполнения операций по диагностике устройства. В правой части окна расположено дерево объектов устройства, с которыми может работать утилита. В нижней части окна отображается процесс выполнения операций утилиты.



Утилита удаленной диагностики. Окно удаленной диагностики устройства

Утилита удаленной диагностики сохраняет загруженные с устройств файлы на рабочем столе устройства, с которого она запущена.

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.

Получение файлов дампа с клиентских устройств с операционной системой Linux не поддерживается.

Чтобы получить файлы дампа с помощью удаленной диагностики, используется утилита kldumper. Эта утилита предназначена для получения файлов дампа процессов приложений "Лаборатории Касперского" по запросу специалистов Службы технической поддержки. Подробная информация о требованиях к использованию утилиты kldumper приведена в Базе знаний Kaspersky Security Center.

Чтобы создать файл дампа для приложения:

1. В рабочей области папки **Управляемые устройства** на вкладке **Устройства** в контекстном меню нужного устройства выберите пункт **Внешние инструменты → Удаленная диагностика**.

   Откроется окно **Утилита удаленной диагностики Kaspersky Security Center**.

2. Подключите утилиту удаленной диагностики к клиентскому устройству.

   В результате откроется окно удаленной диагностики устройства.

3. В правой части окна перейдите по ссылке **Сформировать файл дампа для процесса**.

4. В открывшемся окне **Формирование дампа процесса** укажите исполняемый файл приложения, для которого вы хотите создать файл дампа.

5. Нажмите на кнопку **OK**.

Архив с файлом дампа для указанного приложения загружен.

Если указанное приложение не запущено на клиентском устройстве, папка "result" в загруженном архиве будет пустой.

Если указанное приложение запущено, но загрузка завершается с ошибкой или папка "result" в загруженном архиве пуста, см. Базу знаний Kaspersky Security Center.

Включение и выключение трассировки, загрузка файла трассировки

Чтобы включить трассировку на удаленном устройстве:

1. Запустите утилиту удаленной диагностики и подключитесь к нужному устройству.

2. В дереве объектов устройства выберите приложение, для которого требуется включить трассировку.

   > Включение и выключение трассировки у приложений с самозащитой возможно только при подключении к устройству средствами Сервера администрирования.

   Если вы хотите включить трассировку для Агента администрирования, вы также можете сделать это при создании задачи Установка требуемых обновлений и закрытие уязвимостей. В этом случае Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики.

3. Чтобы включить трассировку:

   a. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Включить трассировку**.

   b. В открывшемся окне **Выбор уровня трассировки** рекомендуется не менять значения, заданные по умолчанию. При необходимости специалист Службы технической поддержки проведет вас через процесс настройки. Доступны следующие параметры:

      - **Уровень трассировки**

        Уровень трассировки определяет состав информации, которую содержит файл трассировки.

- **Трассировка на основе ротации** (доступно только для Kaspersky Endpoint Security)

  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.

c. Нажмите на кнопку **OK**.

4. Для Kaspersky Endpoint Security специалисты Службы технической поддержки могут попросить вас включить трассировку Xperf для получения информации о производительности системы.

   Чтобы включить трассировку xperf:

   a. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Включить трассировку Xperf**.

   b. В открывшемся окне **Выбор уровня трассировки**, в зависимости от запроса специалиста Службы технической поддержки, выберите один из следующих 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.

   c. Выберите один из уровней трассировки:

   - **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.

   d. Также вам могут предложить включить параметр **Трассировка на основе ротации**, 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.

   e. Нажмите на кнопку **OK**.

   В некоторых случаях для включения трассировки приложения безопасности требуется перезапустить это приложение и его задачу.

Утилита удаленной диагностики позволяет получать трассировку для выбранного приложения.

Чтобы загрузить файл трассировки приложения:

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству".
2. В узле приложения в папке **Файлы трассировки** выберите требуемый файл.
3. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Загрузить весь файл**.

   Для файлов большого объема есть возможность загрузить только последние части трассировки.

   Вы можете удалить выделенный файл трассировки. Удаление файла возможно после выключения трассировки.

Выбранный файл загружается в местоположение, указанное в нижней части окна.

Чтобы выключить трассировку на удаленном устройстве:

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству".
2. В дереве объектов устройства выберите приложение, для которого требуется выключить трассировку.

   Включение и выключение трассировки у приложений с самозащитой возможно только при подключении к устройству средствами Сервера администрирования.

3. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Выключить трассировку**.

Утилита удаленной диагностики выключит трассировку для выбранного приложения.

Загрузка параметров приложений

Чтобы загрузить с удаленного устройства параметры приложений:

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству".
2. В дереве объектов окна утилиты удаленной диагностики выберите верхний узел с именем устройства.
3. В левой части окна утилиты удаленной диагностики выберите требуемое действие из следующих параметров:

   - **Загрузить информацию о системе**
   - **Загрузить параметры приложения**
   - **Сформировать файл дампа для процесса**

     В окне, открывшемся по этой ссылке, укажите исполняемый файл приложения, для которого нужно сформировать файл дампа.

- **Запустить утилиту**

  В окне, открывшемся по этой ссылке, укажите исполняемый файл утилиты, которую вы хотите запустить, и параметры ее запуска.

В результате выбранная утилита будет загружена на устройство и запущена на нем.

Загрузка журналов событий

Чтобы загрузить с удаленного устройства журнал событий:

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству".

2. В папке **Журналы событий системы** в дереве объектов устройства выберите соответствующий журнал событий.

3. Чтобы загрузить журнал событий, перейдите по ссылке **Загрузить журнал событий <Имя журнала событий>** в левой части окна утилиты удаленной диагностики.

Выбранный журнал событий загружается в местоположение, указанное в нижней части окна.

Загрузка нескольких диагностических информационных элементов

Утилита удаленной диагностики Kaspersky Security Center позволяет загружать несколько элементов диагностической информации, включая журналы событий, системную информацию, файлы трассировки и файлы дампа.

Чтобы загрузить с удаленного устройства диагностическую информацию:

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству".

2. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Загрузить**.

3. Установите флажки напротив объектов, которые вы хотите загрузить.

4. Нажмите на кнопку **Запустить**.

Каждый выбранный объект загружается в месторасположение, указанное в нижней панели.

Запуск диагностики и загрузка ее результатов

Чтобы запустить диагностику приложения на удаленном устройстве и загрузить ее результаты:

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству".

2. В дереве объектов устройства выберите необходимое приложение.

3. Чтобы запустить диагностику, перейдите по ссылке **Выполнить диагностику** в левой части окна утилиты удаленной диагностики.

   В результате в узле выбранного приложения в дереве объектов появится отчет диагностики.

4. Выберите сформированный отчет диагностики в дереве объектов и скачайте его по ссылке **Папка загрузки**.

Выбранный отчет загружается в местоположение, указанное в нижней части окна.

Запуск, остановка и перезапуск приложений

Запуск, остановка и перезапуск приложений возможны только при подключении к устройству средствами Сервера администрирования.

Чтобы запустить, остановить или перезапустить приложение:

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству".

2. В дереве объектов устройства выберите необходимое приложение.

3. Выберите действие в левой части окна утилиты удаленной диагностики:

   - **Остановить приложение**
   - **Перезапустить приложение**
   - **Запустить приложение**

В зависимости от выбранного вами действия приложение запустится, остановится или перезапустится.

Устройства с защитой на уровне UEFI

Устройство с защитой на уровне UEFI – это устройство со встроенным на уровне BIOS решением или приложением "Лаборатории 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 безопасности. Kaspersky Security Center поддерживает управление такими устройствами.

Чтобы изменить параметры подключения устройств с защитой на уровне UEFI:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.

2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

3. В окне свойств Сервера администрирования выберите раздел **Параметры подключения к Серверу** → **Дополнительные порты**.

4. В разделе **Дополнительные порты** измените необходимые вам параметры:

   - **Открыть порт для устройств с защитой на уровне UEFI и устройств с KasperskyOS**

     Если флажок установлен, то устройства с защитой на уровне UEFI могут подключаться к Серверу администрирования.

     По умолчанию флажок установлен.

   - **Порт для устройств с защитой на уровне UEFI и устройств с KasperskyOS**

     Вы можете изменить номер порта, если установлен флажок **Открыть порт для устройств с защитой на уровне UEFI**. По умолчанию используется порт 13294.

5. Нажмите на кнопку **OK**.

Параметры управляемого устройства

Чтобы просмотреть параметры управляемого устройства:

1. В дереве консоли выберите папку **Управляемые устройства**.
2. В рабочей области папки выберите устройство.
3. В контекстном меню устройства выберите пункт **Свойства**.

Откроется окно свойств устройства с выбранным разделом **Общие**.

Общие.

Раздел **Общие** содержит общую информацию о клиентском устройстве. Информация предоставляется на основании данных, полученных в ходе последней синхронизации клиентского устройства с Сервером администрирования:

- **Имя**

  В поле можно просмотреть и изменить имя клиентского устройства в группе администрирования.

- **Описание**

  В поле можно ввести дополнительное описание клиентского устройства.

- **Windows-домен**

  Windows-домен или рабочая группа, в которую входит устройство.

- **NetBIOS-имя**

  Имя клиентского устройства в сети Windows.

- **DNS-имя**

  Имя DNS-домена клиентского устройства.

- **IP-адрес**

  IP-адрес устройства

- **Группа**

  Группа администрирования, в состав которой входит клиентское устройство.

- **Последнее обновление**

  Дата последнего обновления антивирусных баз или приложений на устройстве.

- **Последнее появление в сети**

  Дата и время, когда устройство последний раз было видимо в сети.

- **Соединение с Сервером администрирования**

  Дата и время последнего соединения Агента администрирования, установленного на клиентском устройстве, с Сервером администрирования.

- **Не разрывать соединение с Сервером администрирования**

  Если этот параметр включен, сохраняется постоянное соединение между управляемым устройством и Сервером администрирования. Вы можете использовать этот параметр, если не используете push-серверы, которые обеспечивают такое соединение.

  Если параметр выключен и push-серверы не используются, управляемое устройство подключается к Серверу администрирования для синхронизации данных или передачи информации.

  Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

  Этот параметр по умолчанию выключен на управляемых устройствах. Этот параметр включен по умолчанию на устройстве, на котором установлен Сервер администрирования, и остается включенным, даже если вы попытаетесь его выключить.

Защита.

В разделе **Защита** представлена информация о состоянии антивирусной защиты на клиентском устройстве:

- **Статус устройства**

  Статус клиентского устройства, формируемый на основании установленных администратором критериев состояния антивирусной защиты на устройстве и активности устройства в сети.

- **Все проблемы**

  Эта таблица содержит полный список проблем, обнаруженных управляемыми приложениями, установленных на клиентском устройстве. Каждая проблема имеет статус, который управляемое приложение предлагает вам назначить устройству из-за этой проблемы.

- **Постоянная защита**

  Статус текущего состояния постоянной защиты клиентского устройства.

  После того как статус изменяется на устройстве, новый статус отображается в окне свойств устройства только после синхронизации клиентского устройства с Сервером администрирования.

- **Последняя проверка по требованию**

  Дата и время последнего поиска вредоносного ПО на клиентском устройстве.

- **Всего обнаружено угроз**

  Общее количество обнаруженных на клиентском устройстве угроз с момента установки приложения безопасности (первой проверки устройства) либо с момента последнего обнуления счетчика угроз.

- **Активные угрозы**

  Количество необработанных файлов на клиентском устройстве.

  В поле не учитывается количество необработанных файлов для мобильных устройств.

- **Статус шифрования дисков**

  Текущее состояние шифрования файлов на локальных дисках устройства. Описание статусов см. в онлайн-справке Kaspersky Endpoint Security для Windows.

Приложения

В разделе **Приложения** отображается список приложений "Лаборатории Касперского", установленных на клиентском устройстве. В этом разделе находится кнопка запуска () и кнопка остановки (), позволяющая запускать и останавливать выбранное приложение "Лаборатории Касперского" (кроме Агента администрирования). Эти кнопки доступны, если на управляемых устройствах доступен порт 15000 UDP для приема push-уведомлений от Сервера 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 запуска и остановки активны. Также раздел **Приложения** содержит следующие кнопки:

- **События**

  При нажатии на кнопку можно просмотреть список событий, произошедших на клиентском устройстве при работе программы, а также результаты выполнения задач для этой программы.

- **Статистика**

  При нажатии на кнопку можно просмотреть текущую статистическую информацию о работе программы.

- **Свойства**

  При нажатии на кнопку можно получить информацию о программе и выполнить настройку программы.

Tasks

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.

Кнопки запуска (), остановки () и удаления () доступны, если на управляемых устройствах доступен порт 15000 UDP для приема push-уведомлений от Сервера 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 запуска, остановки и удаления активны.

При отсутствии подключения статус задачи 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.

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.

Информация о системе

В разделе **Общая информация о системе** представлена информация о программе, установленной на клиентском устройстве.

Реестр приложений

В разделе **Реестр приложений** 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**.

- **Показывать только несовместимые приложения безопасности**

  Если флажок установлен, в списке программ отображаются только те программы безопасности, которые несовместимы с программами "Лаборатории Касперского".

  По умолчанию флажок снят.

- **Показывать обновления**

  Если флажок установлен, в списке программ отображаются не только программы, но и установленные для них пакеты обновлений.

  По умолчанию флажок снят.

- **Экспортировать в файл**

  Нажмите эту кнопку, чтобы экспортировать список приложений, установленных на устройстве, в файл формата CSV или TXT.

- **История**

  Нажмите эту кнопку, чтобы просмотреть события, относящиеся к установке приложений на устройство. Отобразится следующая информация:

  - дата и время, когда приложение было установлено на устройство;
  - название приложения;
  - Версия приложения.

- **Свойства**

  Нажмите эту кнопку, чтобы просмотреть свойства приложения, выбранного в списке приложений, установленных на устройстве. Отобразится следующая информация:

  - название приложения;
  - версия приложения;
  - поставщик приложения.

Исполняемые файлы

В разделе **Исполняемые файлы** отображаются исполняемые файлы, обнаруженные на клиентском устройстве.

О реестре оборудования

В разделе **Реестр оборудования** можно просмотреть информацию об оборудовании, установленном на клиентском устройстве. Эту информацию можно просматривать для устройств я операционными системами Windows и Linux.

Убедитесь, что утилита lshw установлена на устройствах Linux, с которых вы хотите получить информацию об оборудовании. Сведения об оборудовании, полученные с виртуальных машин, могут быть неполными в зависимости от используемого гипервизора

Если 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.

Сеансы

В разделе **Сеансы** представлена информация о владельце клиентского устройства, а также об учетных записях пользователей, которые работали с выбранным клиентским устройством.

Информация о доменных пользователях формируется на основе данных Active Directory. Информация о локальных пользователях предоставляется Диспетчером учетных записей безопасности (Security Account Manager), установленным на клиентском устройстве.

- **Владелец устройства**

  В поле **Владелец устройства** отображается имя пользователя, с которым администратор может контактировать в случае необходимости выполнить какие-либо работы с клиентским устройством.

  По кнопкам **Назначить** и **Свойства** можно выбрать владельца устройства и просмотреть информацию о пользователе, назначенном владельцем устройства.

  По кнопке с красным крестом можно удалить текущего владельца устройства.

В списке содержатся учетные записи пользователей, которые работают с клиентским устройством.

- **Имя**

  Имя устройства в Windows-сети.

- **Имя участника**

  Имя пользователя (доменное или локальное), который выполнил вход в систему на этом устройстве.

- **Учетная запись**

  Учетная запись пользователя, который выполнил вход в систему на этом устройстве.

- **Электронная почта**

  Адреса электронной почты пользователя.

- **Телефон**

  Номер телефона пользователя.

Проблемы безопасности

На вкладке **Проблемы безопасности** можно просматривать, изменять и создавать проблемы безопасности для клиентского устройства. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором. Например, если пользователь постоянно переносит на устройство вредоносные приложения с личного съемного диска, администратор может создать проблему безопасности. Администратор может указать краткое описание случая и рекомендуемых действий (таких как дисциплинарные действия), которые должны быть предприняты против пользователя в тексте проблемы безопасности, и может добавить ссылку на пользователя или пользователей.

Проблема безопасности, для которой выполнены необходимые действия, называется *обработанным*. Наличие необработанных проблем безопасности может быть выбрано условием для изменения статуса устройства на *Критический* или *Предупреждение*.

В разделе содержится список проблем безопасности, созданных для устройства. Проблемы безопасности классифицируются по уровню важности и типу. Тип проблемы безопасности определяется приложением "Лаборатории Касперского", которое создает проблему безопасности. Обработанные проблемы безопасности можно отметить в списке, установив флажок в столбце **Обработана**.

Уязвимости в приложениях

В разделе **Уязвимости в программах** можно просмотреть список с информацией об уязвимостях сторонних программ, установленных на клиентских устройствах. С помощью строки поиска над списком вы можете искать в списке уязвимости по имени уязвимости.

- **Экспортировать в файл**

  По кнопке **Экспортировать в файл** вы можете сохранить список уязвимостей в файле. По умолчанию приложение экспортирует список уязвимостей в файл формата CSV.

- **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**

  Выберите уязвимость в приложениях в списке и нажмите на кнопку **Свойства**, 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 Web Console).
  - Просмотреть список рекомендуемых исправлений для уязвимости.
  - Вручную указать обновления программного обеспечения для закрытия уязвимости (в Консоли администрирования или в Kaspersky Security Center Web Console).
  - Просмотреть экземпляр уязвимости.
  - Просмотреть список существующих задач для закрытия уязвимости и создать задачи для закрытия уязвимости.

Применимые обновления

В этом разделе можно просмотреть список обнаруженных на устройстве обновлений программного обеспечения, которые не были установлены. Информация о необязательных обновлениях Microsoft Windows не отправляется на Сервер администрирования.

- **Показывать установленные обновления**

  Если параметр включен, в списке обновлений отображаются и не установленные обновления, и обновления, которые уже установлены на клиентском устройстве.

  По умолчанию параметр выключен.

Активные политики

В этом разделе отображается список политик для приложений "Лаборатории Касперского", назначенных в настоящее время этому устройству.

- **Экспортировать в файл**

  По кнопке **Экспортировать в файл** вы можете сохранить список активных политик в файле. По умолчанию приложение экспортирует список политик в файл формата CSV.

Действующие профили политик

- **Действующие профили политик**

  В списке можно просмотреть информацию о действующих профилях политики, которые активны на клиентских устройствах. С помощью строки поиска над списком вы можете искать в списке действующие профили политик по имени политики или по имени профиля политики.

- **Экспортировать в файл**

  По кнопке **Экспортировать в файл** вы можете сохранить список активных профилей политики в файле. По умолчанию приложение экспортирует список профилей политики в файл формата CSV.

Точки распространения

В этом разделе представлен список агентов обновлений, 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.

Общие параметры политик

Общие

В разделе **Общие** можно изменить состояние политики и настроить наследование параметров политики.

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:

  - **Активная политика**

    Если выбран этот вариант, политика становится активной.

    По умолчанию выбран этот вариант.

  - **Политика для автономных пользователей**

    Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.

- **Неактивная политика**

  Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.

- В блоке **Наследование параметров** можно настроить параметры наследования политики:

  - **Наследовать параметры родительской политики**

    Если параметр включен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

    По умолчанию параметр включен.

  - **Обеспечить принудительное наследование параметров для дочерних политик**

    Если параметр включен, после применения изменений в политике будут выполнены следующие действия:

    - значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
    - в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически включен параметр **Наследовать параметры родительской политики**.

    Когда параметр включен, значения параметров дочерних политик недоступны для изменения.

    По умолчанию параметр выключен.

Настройка событий

В разделе **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на закладках:

- **Отказ функционирования**.
- **Предупреждение**.
- **Информационное сообщение**.

В списке 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.

Для выбора нескольких типов событий используйте клавиши **SHIFT** или **CTRL**, для выбора всех типов используйте кнопку **Выбрать все**.

Параметры политики Агента администрирования

Чтобы настроить параметры политики Агента администрирования:

1. В дереве консоли выберите папку **Политики**.
2. В рабочей области папки выберите политику Агента администрирования.
3. В контекстном меню политики выберите пункт **Свойства**.

Откроется окно свойств политики Агента администрирования.

> См. таблицу сравнения, в которой подробно описано применение параметров, описанных ниже, в зависимости от используемой операционной системы.

Общие

В разделе **Общие** можно изменить состояние политики и настроить наследование параметров политики.

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:
  - **Активная политика**

    Если выбран этот вариант, политика становится активной.

    По умолчанию выбран этот вариант.
  - **Политика для автономных пользователей**

    Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.
  - **Неактивная политика**

    Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.
- В блоке **Наследование параметров** можно настроить параметры наследования политики:
  - **Наследовать параметры родительской политики**

    Если параметр включен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

    По умолчанию параметр включен.
  - **Обеспечить принудительное наследование параметров для дочерних политик**

    Если параметр включен, после применения изменений в политике будут выполнены следующие действия:
    - значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
    - в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически включен параметр **Наследовать параметры родительской политики**.

Когда параметр включен, значения параметров дочерних политик недоступны для изменения.

По умолчанию параметр выключен.

Настройка событий

В разделе **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на закладках:

- **Отказ функционирования**.
- **Предупреждение**.
- **Информационное сообщение**.

В списке 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.

Для выбора нескольких типов событий используйте клавиши **SHIFT** или **CTRL**, для выбора всех типов используйте кнопку **Выбрать все**.

Settings

В разделе **Параметры** можно настроить параметры политики Агента администрирования:

- **Распространять файлы только через точки распространения**

  Если этот параметр включен, Агенты администрирования на управляемых устройствах получают обновления только от точек распространения.

  Если этот параметр выключен, Агенты администрирования на управляемых устройствах получают обновления от точек распространения или от Сервера администрирования.

  > Обратите внимание, что приложения безопасности на управляемых устройствах получают обновления от источника, заданного в задаче обновления для каждого приложения безопасности. Если вы включили параметр **Распространять файлы только через точки распространения**, убедитесь, что Kaspersky Security Center установлен в качестве источника обновлений в задачах обновления.

  По умолчанию параметр выключен.

- **Максимальный размер очереди событий (МБ)**

  В поле можно указать максимальное место на диске, которое может занимать очередь событий.

  По умолчанию указано значение 2 МБ.

- **Приложение может получать расширенные данные политики на устройстве**

  Агент администрирования, установленный на управляемом устройстве, передает информацию о применяемой политике в приложение безопасности (например, Kaspersky Endpoint Security для 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.

  По умолчанию параметр выключен.

Хранилища

В разделе **Хранилища** можно выбрать типы объектов, информацию о которых Агент администрирования будет отправлять на Сервер администрирования:

- **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**

  Установленный на устройстве Агент администрирования отправляет информацию об оборудовании устройства на Сервер администрирования. Вы можете просмотреть информацию об оборудовании в свойствах устройства.

  Убедитесь, что утилита lshw установлена на устройствах Linux, с которых вы хотите получить информацию об оборудовании. Сведения об оборудовании, полученные с виртуальных машин, могут быть неполными в зависимости от используемого гипервизора

- **Информация об установленных приложениях**

  Если этот параметр включен, на Сервер администрирования отправляется информация о приложениях, установленных на клиентских устройствах.

  По умолчанию параметр включен.

- **Включить информацию о патчах**

  Информация о патчах приложений, установленных на клиентских устройствах, отправляется на Сервер администрирования. Включение этого параметра может увеличить нагрузку на Сервер администрирования и СУБД, а также вызвать увеличение объема базы данных.

  По умолчанию параметр включен. Доступен только для Windows.

Если в политике Агента администрирования наложен запрет на изменение параметров, указанных в этом разделе, эти параметры недоступны для изменения.

Обновления и уязвимости в приложениях

В разделе **Обновления и уязвимости в приложениях** можно настроить поиск и распространение обновлений Windows, а также включить проверку исполняемых файлов на наличие уязвимостей:

- **Использовать Сервер администрирования в роли WSUS-сервера**

  Если этот параметр включен, обновления Windows загружаются на Сервер администрирования. Загруженные обновления Сервер администрирования централизованно предоставляет службам Windows Update на клиентских устройствах с помощью Агентов администрирования.

  Если этот параметр выключен, Сервер администрирования не используется для загрузки обновлений Windows. В этом случае клиентские устройства получают обновления Windows самостоятельно.

  По умолчанию параметр выключен.

- С помощью параметра **Разрешить пользователям управлять установкой обновлений Центра обновления Windows** вы можете ограничить обновления Windows, которые пользователи могут устанавливать на своих устройствах вручную, с помощью Центра обновления Windows.

  Для устройств с операционными системами Windows 10, если в Центре обновления Windows уже найдены обновления для устройств, то новый параметр, который вы выбрали под **Разрешить пользователям управлять установкой обновлений Центра обновления Windows**, будет применен только после установки найденных обновлений.

  Выберите параметр из раскрывающегося списка:

  - **Устанавливать все применимые обновления Центра обновления Windows**

    Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам.

    Выберите этот вариант, если вы не хотите влиять на установку обновлений.

    Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

  - **Устанавливать только одобренные обновления Центра обновления Windows**

    Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам и которые одобрены администратором.

    Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом разрешить установку этих одобренных обновлений на клиентских устройствах.

    Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

  - **Запретить устанавливать обновления Центра обновления Windows**

    Пользователи не могут устанавливать обновления Центра обновления Windows на своих устройства вручную. Все применимые обновления устанавливаются в соответствии с настройкой, заданной администратором.

    Выберите этот вариант, если вы хотите централизованно управлять установкой обновлений.

    Например, вы можете настроить расписание обновления так, чтобы не загружать сеть. Вы можете запланировать обновления вне рабочего времени, чтобы они не мешали производительности пользователей.

- 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 включен.

Управление перезагрузкой

В разделе **Управление перезагрузкой** можно выбрать и настроить действие, если во время работы, установки или удаления приложения требуется перезагрузить операционную систему управляемого устройства:

- **Не перезагружать операционную систему**

  Перезагрузка операционной системы не выполняется.

  Этот вариант выбран по умолчанию.

- **При необходимости перезагрузить операционную систему автоматически**

  При необходимости перезагрузка операционной системы выполняется автоматически.

- **Запрашивать у пользователя**

  Программа запрашивает у пользователя разрешение перезагрузить операционную систему.

  - **Повторять запрос периодически через (мин)**

    Если флажок установлен, программа запрашивает у пользователя разрешение на перезагрузку операционной системы с периодичностью, указанной в поле рядом с флажком. По умолчанию периодичность повторных запросов составляет 5 минут.

    Если флажок снят, программа не запрашивает разрешение на перезагрузку повторно.

    По умолчанию флажок установлен.

  - **Принудительно перезагружать через (мин)**

    Если флажок установлен, после запроса у пользователя операционная система перезагружается принудительно по истечении времени, указанного в поле рядом с флажком.

    Если флажок снят, принудительная перезагрузка не выполняется.

    По умолчанию флажок снят.

  - **Время ожидания перед принудительным закрытием приложения в заблокированных сессиях через (мин)**

    Принудительное завершение работы приложений, когда устройство пользователя заблокировано (автоматически после периода неактивности или вручную).

    Если параметр включен, работа приложений на заблокированном устройстве принудительно прекращается по истечении времени, указанного в поле ввода.

    Если параметр выключен, работа приложений на заблокированном устройстве не прекращается.

    По умолчанию параметр выключен.

Совместный доступ к рабочему столу Windows

В разделе **Общий доступ к рабочему столу** можно включить и настроить аудит действий администратора на удаленном устройстве пользователя при использовании общего доступа к рабочему столу:

- **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.

  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:

- **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**

  Если флажок установлен, патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений.

  Если флажок снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрен*.

  По умолчанию параметр включен.

- **Загружать обновления и антивирусные базы с Сервера администрирования заранее (рекомендуется)**

  Если параметр включен, офлайн-модель получения обновлений используется. Когда Сервер администрирования получает обновления, он уведомляет Агент администрирования (на устройствах, где он установлен) об обновлениях, которые потребуются для управляемых приложений. Когда Агенты администрирования получают информацию об обновлениях, они загружают нужные файлы с Сервера администрирования заранее. При первом соединении с Агентом администрирования Сервер инициирует загрузку обновлений этим Агентом. После того как Агент администрирования на клиентском устройстве загрузит все обновления, обновления становятся доступными для приложений на устройстве.

  Когда управляемое приложение на клиентском устройстве обращается к Агенту администрирования за обновлениями, Агент проверяет, есть ли у него необходимые обновления. Если обновления были получены от Сервера администрирования не раньше, чем за 25 часов с момента запроса управляемого приложения, Агент администрирования не подключается к Серверу администрирования и предоставляет управляемому приложению обновления из локального кеша. Соединение с Сервером администрирования может не выполняться, когда Агент администрирования предоставляет обновления для приложений на клиентских устройствах, но подключение не требуется для обновления.

  Если параметр выключен, офлайн-модель получения обновлений не используется. Обновления распространяются в соответствии с расписанием задачи загрузки обновлений.

  По умолчанию параметр включен.

Подключения.

Раздел **Подключения** включает три вложенных раздела:

- **Сеть**
- **Профили соединений** (только для Windows и macOS)
- **Расписание соединений**

В разделе **Сеть** можно настроить параметры подключения к Серверу администрирования, включить возможность использования UDP-порта и указать его номер. Доступны следующие параметры:

- В блоке **Подключение к Серверу администрирования** можно настроить параметры подключения к Серверу администрирования и указать период синхронизации клиентских устройств с Сервером администрирования:
  - **Сжимать сетевой трафик**

    Если параметр выключен, будет увеличена скорость передачи данных Агентом администрирования, сокращен объем передаваемой информации и уменьшена нагрузка на Сервер администрирования.

    > Нагрузка на центральный процессор клиентского компьютера может возрасти.

    По умолчанию флажок установлен.
  - **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**

    Если параметр включен, порты, необходимые для работы Агента администрирования, будут добавлены в список исключений брандмауэра Microsoft Windows.

    По умолчанию параметр включен.
  - **Использовать SSL**

    Если этот параметр включен, подключение к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

    По умолчанию параметр включен.
  - **Использовать шлюз соединения точки распространения (при наличии) в параметрах подключения по умолчанию**

    Если параметр включен, то используется шлюз соединений точки распространения, параметры которой заданы в свойствах группы администрирования.

    По умолчанию параметр включен.
- **Использовать UDP-порт**

  Чтобы Агент администрирования подключался к Серверу администрирования через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **Номер UDP-порт** укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к Серверу администрирования выполняется через UDP-порт 15000.

- **Номер UDP-порта**

  В поле можно ввести номер UDP-порта. По умолчанию установлен порт 15000.

  Используется десятичная форма записи.

  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 вы выбрали параметр **Использовать эту точку распространения в качестве push-сервера** в окне параметров точки распространения. Иначе точка распространения не будет выполнять роль push-сервера.

В разделе **Профили соединений** можно задать параметры сетевого местоположения, настроить профили подключения к Серверу администрирования, включить автономный режим, когда Сервер администрирования недоступен.

- **Параметры сетевого местоположения**

  Параметры сетевого местоположения определяют характеристики сети, к которой подключено клиентское устройство, и задают правила переключения Агента администрирования с одного профиля подключения Сервера администрирования на другой при изменении характеристик сети.

- **Профили подключения к Серверу администрирования**

  В этом разделе можно просмотреть и добавить профили подключения Агента администрирования к Серверу администрирования. В этом разделе также можно сформировать правила переключения Агента администрирования на другие Серверы администрирования при возникновении следующих событий:

  - подключении клиентского устройства к другой локальной сети;
  - отключении устройства от локальной сети организации;
  - изменении адреса шлюза соединения или изменении адреса DNS-сервера.

  > Профили подключения поддерживаются только для устройств под управлением Windows и macOS.

- **Включить автономный режим, когда Сервер администрирования недоступен**

  Если параметр включен, при подключении через этот профиль приложения, установленные на клиентском устройстве, будут использовать профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей. В случае, если для приложения политика для автономных пользователей не определена, приложение будет использовать активную политику.

  Если параметр выключен, приложения будут использовать активные политики.

  По умолчанию параметр выключен.

В разделе **Расписание соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования:

- **Подключаться при необходимости**

  Если выбран этот вариант, подключение будет устанавливаться тогда, когда Агенту администрирования нужно передать данные на Сервер администрирования.

  По умолчанию выбран этот вариант.

- **Подключаться в указанные периоды**

  Если выбран этот вариант, подключение Агента администрирования к Серверу администрирования выполняется в заданные периоды времени. Можно добавить несколько периодов подключения.

Точки распространения

Раздел **Точки распространения** включает четыре вложенных раздела:

- **Опросы сети**
- **Параметры подключения к интернету**
- **Прокси-сервер KSN**
- **Обновления**

В подразделе **Опросы сети** вы можете настроить автоматический опрос сети. Вы можете включить три типа опроса, то есть опрос сети, опрос IP-диапазонов и опрос Active Directory:

- **Разрешить опрос сети**

  Если этот параметр включен, Сервер администрирования автоматически опрашивает сеть в соответствии с расписанием, настроенным по ссылкам **Настроить расписание быстрого опроса** и **Настроить расписание полного опроса**.

  Если этот параметр выключен, Сервер администрирования опрашивает сеть с указанным периодом в поле **Период опроса сети (мин)**.

  Период обнаружения устройств для версий Агента администрирования ниже 10.2 можно настроить в полях **Период опроса Windows-доменов (мин)** (для быстрого опроса сети Windows) и **Период опроса сети (мин)** (для полного опроса сети Windows).

  По умолчанию параметр выключен.

- **Разрешить опрос IP-диапазона**

  Если этот параметр включен, точка распространения автоматически опрашивает IP-диапазоны в соответствии с расписанием, настроенным по кнопке **Настроить расписание опроса**.

  Если параметр выключен, точка распространения не выполняет опрос IP-диапазонов.

  Периодичность опроса IP-диапазонов для версий Агента администрирования версий ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если параметр включен.

  По умолчанию параметр выключен.

- **Использовать опрос Zeroconf (только для платформ Linux; указанные вручную IP-диапазоны игнорируются)**

  Если этот параметр включен, точка распространения автоматически опрашивает сеть с устройствами IPv6, используя сеть с нулевой конфигурацией (далее также *Zeroconf*). В этом случае включенный опрос IP-диапазонов игнорируется, так как точка распространения опрашивает всю сеть.

  Чтобы можно было начать использовать Zeroconf, должны быть выполнены следующие условия:

  - Точка распространения должна работать под управлением Linux.
  - Вам нужно установить утилиту avahi-browse на точку распространения.

Если этот параметр отключен, точка распространения не опрашивает сети с устройствами IPv6.

По умолчанию параметр выключен.

- **Разрешить опрос Active Directory**

  Если этот параметр включен, точка администрирования автоматически выполняет опрос Active Directory в соответствии с расписанием, настроенным по ссылке **Настроить расписание опроса**.

  Если параметр выключен, Сервер администрирования не выполняет опрос Active Directory.

  Периодичность опроса Active Directory для версий Агента администрирования версий ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если этот параметр включен.

  По умолчанию параметр выключен.

Если ваши точки распространения используют прокси-сервер для подключения к интернету, в подразделе **Параметры подключения к интернету** вы можете указать следующие параметры:

- **Использовать прокси-сервер**

  Если этот флажок установлен, для подключения точек распространения к серверу обновлений "Лаборатории Касперского" используется прокси-сервер в интернете. Вы можете настроить подключение к прокси-серверу в полях ввода.

  По умолчанию флажок снят.

- **Адрес прокси-сервера**

  Адрес прокси-сервера.

- **Номер порта**

  Номер порта, по которому будет выполняться подключение.

- **Не использовать прокси-сервер для локальных адресов**

  Если параметр включен, то при подключении к устройствам в локальной сети не используется прокси-сервер.

  По умолчанию параметр выключен.

- **Аутентификация на прокси-сервере**

  Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  По умолчанию флажок снят.

- **Имя пользователя**

  Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.

- **Пароль**

  Пароль учетной записи, от имени которой будет запускаться задача.

В разделе **Прокси-сервер KSN** вы можете настроить приложение так, чтобы точка распространения использовалась для пересылки KSN запросов от управляемых устройств:

- **Включить прокси-сервер KSN на стороне точки распространения**

  Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

  Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского".

  По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены в окне свойств Сервера администрирования.

  Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

- **Пересылать KSN запрос Серверу администрирования**

  Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

  По умолчанию параметр включен.

- **Доступ к облачной службе KSN/KPSN непосредственно через интернет**

  Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или KPSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или KPSN.

  Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к KPSN. Если вы хотите перенастроить точки распространения для отправки запросов KSN в KPSN, включите параметр **Пересылать KSN запрос Серверу администрирования** для каждой точки распространения.

  Точки распространения с установленным Агентом администрирования версии 12 (и выше) могут напрямую обращаться к KPSN.

- **TCP-порт**

  Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.

- **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.

В подразделе **Обновления** вы можете указать, должен ли Агент администрирования загружать файлы различий, включив или выключив параметр **Загрузить файлы различий**. (По умолчанию параметр включен.)

История ревизий

В этом разделе можно посмотреть историю ревизий Агента администрирования. Вы можете сравнивать ревизии, просматривать ревизии, сохранять ревизии в файл, добавлять и изменять описания ревизий.

Управление учетными записями пользователей

Этот раздел содержит информацию об учетных записях и ролях пользователей, которые поддерживает приложение. В разделе приведены инструкции по созданию учетных записей и ролей пользователей Kaspersky Security Center.

Kaspersky Security Center 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. Вы можете создавать учетные записи внутренних пользователей. Эти учетные записи используются только в Kaspersky Security Center.

Работа с учетными записями пользователей

Kaspersky Security Center позволяет управлять учетными записями пользователей и группами учетных записей. Приложение поддерживает два типа учетных записей:

- Учетные записи сотрудников организации. Сервер администрирования получает данные об учетных записях этих пользователей при опросе сети организации.
- Учетные записи внутренних пользователей. Применяются для работы с виртуальными Серверами администрирования. Учетные записи внутренних пользователей создаются и используются только внутри Kaspersky Security Center.

Вы можете просмотреть список учетных записей пользователей одним из следующих способов:

- В дереве консоли перейдите в раздел **Дополнительно** → **Учетные записи пользователей**.
- В дереве консоли перейдите в папку **Управляемые устройства** → вкладка **Устройства** → ссылка <название устройства> → раздел **Сеансы**.

  В разделе **Сеансы** отображаются учетные записи пользователей с активными сеансами на устройствах под управлением Windows.

Список учетных записей пользователей отображается правильно, если выполнены следующие требования:

- Используется Агент администрирования той же версии, что и Сервер администрирования, или выше.
- Опрос Active Directory включен для отображения учетных записей пользователей домена.
- На управляемых устройствах под управлением Windows работает служба **Сервера (LanmanServer)**.

Вы можете выполнять с учетными записями пользователей и группами учетных записей следующие действия:

- настраивать права доступа пользователей к функциям приложения с помощью ролей;
- рассылать сообщения пользователям с помощью электронной почты и SMS;
- просматривать список мобильных устройств пользователя;
- выписывать и устанавливать сертификаты на мобильные устройства пользователя;
- просматривать список сертификатов, выписанных пользователю;
- выключать двухфакторную аутентификацию для учетной записи пользователя.

Добавление учетной записи внутреннего пользователя

Чтобы добавить новую учетную запись пользователя Kaspersky Security Center:

1. В дереве консоли откройте папку **Учетные записи пользователей**.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В рабочей области нажмите на кнопку **Добавить пользователя**.

3. В открывшемся окне **Новый пользователь** укажите параметры нового пользователя:

   - Имя пользователя ().

     > Пожалуйста, будьте внимательны при вводе имени пользователя. Вы не сможете его изменить после сохранения изменений.

   - **Описание**
   - **Полное имя**
   - **Основная электронная почта**
   - **Основной телефон**
   - **Пароль** для подключения пользователя к Kaspersky Security Center

     Пароль должен соответствовать следующим правилам:

     - Длина пароля должна быть от 8 до 256 символов.
     - Пароль должен содержать символы как минимум трех групп из списка ниже:
       - верхний регистр (A–Z);
       - нижний регистр (a–z);

- числа (0–9);
- специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).

- Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", если "." расположена перед "@".

Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

Количество попыток ввода пароля пользователем ограничено. По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить максимальное количество попыток ввода пароля, как описано в разделе "Изменение количества попыток ввода пароля".

Если пользователь неправильно ввел пароль заданное количество раз, учетная запись пользователя блокируется на один час. В списке учетных записей пользователей значок () заблокированной учетной записи затемнен (недоступен). Вы можете разблокировать учетную запись, только сменив пароль.

- При необходимости установите флажок **Отключить учетную запись**, чтобы запретить пользователю подключаться к приложению. Например, можно отключить учетную запись, если вы хотите создать учетную запись заранее, но активировать ее позже.
- Установите флажок **Запрашивать пароль при изменении параметров учетной записи**, если вы хотите включить дополнительную защиту учетной записи пользователя от несанкционированного изменения. Если этот параметр включен, то для изменения параметров учетной записи пользователя требуется авторизация пользователя с правом Изменение списков управления доступом объектов в области **Общие функции: Права пользователей**.

4. Нажмите на кнопку **OK**.

Созданная учетная запись пользователя отобразится в рабочей области папки **Учетные записи пользователей**.

Изменение учетной записи внутреннего пользователя

Чтобы изменить учетную запись внутреннего пользователя Kaspersky Security Center:

1. В дереве консоли откройте папку **Учетные записи пользователей**.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В рабочей области дважды нажмите на учетную запись внутреннего пользователя, которую требуется изменить.

3. В открывшемся окне **Свойства: <имя пользователя>** измените параметры учетной записи пользователя:

   - **Описание**
   - **Полное имя**
   - **Основная электронная почта**

- **Основной телефон**
- **Пароль** для подключения пользователя к Kaspersky Security Center

  Пароль должен соответствовать следующим правилам:

  - Длина пароля должна быть от 8 до 256 символов.
  - Пароль должен содержать символы как минимум трех групп из списка ниже:
    - верхний регистр (A–Z);
    - нижний регистр (a–z);
    - числа (0–9);
    - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
  - Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", если "." расположена перед "@".

  Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

  Количество попыток ввода пароля пользователем ограничено. По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить максимальное количество попыток ввода пароля, как описано в разделе "Изменение количества попыток ввода пароля".

  Если пользователь неправильно ввел пароль заданное количество раз, учетная запись пользователя блокируется на один час. В списке учетных записей пользователей значок () заблокированной учетной записи затемнен (недоступен). Вы можете разблокировать учетную запись, только сменив пароль.

- При необходимости установите флажок **Отключить учетную запись**, чтобы запретить пользователю подключаться к приложению. Например, можно отключить учетную запись после того, как сотрудник увольняется из компании.
- Выберите параметр **Запрашивать пароль при изменении параметров учетной записи**, если вы хотите включить дополнительную защиту учетной записи пользователя от несанкционированного изменения. Если этот параметр включен, то для изменения параметров учетной записи пользователя требуется авторизация пользователя с правом Изменение списков управления доступом объектов в области **Общие функции: Права пользователей**.

4. Нажмите на кнопку **ОК**.

Измененная учетная запись пользователя отобразится в рабочей области папки **Учетные записи пользователей**.

Изменение количества попыток ввода пароля

Пользователь Kaspersky Security Center может вводить неверный пароль ограниченное количество раз. После этого учетная запись пользователя блокируется на час.

По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить количество попыток ввода пароля, следуя инструкции ниже.

Чтобы изменить количество попыток ввода пароля:

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск → Выполнить**.

2. Перейдите к следующему разделу:

   - для 32-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

   - для 64-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF

3. Если параметр SrvSplPpcLogonAttempts отсутствует в разделе реестра, создайте его. Тип значения параметра – DWORD.

   Этот параметр не создается по умолчанию при установке Kaspersky Security Center.

4. Укажите требуемое количество попыток в качестве значения параметра SrvSplPpcLogonAttempts.

5. Нажмите на кнопку **OK**, чтобы сохранить изменения.

6. Перезапустите службу Сервера администрирования.

Максимальное количество попыток ввода пароля изменено.

Настройка проверки уникальности имени внутреннего пользователя

Вы можете настроить проверку уникальности имени внутреннего пользователя Kaspersky Security Center при его добавлении в приложение. Проверка на уникальность имени внутреннего пользователя может выполняться только на виртуальном Сервере или главном Сервере, для которого создается учетная запись пользователя, или на всех виртуальных Серверах и главном Сервере. По умолчанию проверка на уникальность имени внутреннего пользователя выполняется на всех виртуальных Серверах и на главном Сервере администрирования.

Чтобы включить проверку уникальности имени внутреннего пользователя в рамках виртуального Сервера или главного Сервера:

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск → Выполнить**.

2. Перейдите в раздел:

   - для 32-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

   - для 64-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

3. Для ключа LP_InterUserUniqVsScope (DWORD) установите значение 00000001.

   По умолчанию для этого ключа указано значение 0.

4. Перезапустите службу Сервера администрирования.

В результате проверка уникальности имени будет выполнена только на том виртуальном Сервере, на котором был создан внутренний пользователь, или на главном Сервере, если пользователь был создан на главном Сервере.

Чтобы включить проверку уникальности имени внутреннего пользователя на всех виртуальных Серверах и главном Сервере:

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск → Выполнить**.

2. Перейдите в раздел:

   - для 64-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

   - для 32-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

3. Для ключа LP_InterUserUniqVsScope (DWORD) установите значение 00000000.

   По умолчанию для этого ключа указано значение 0.

4. Перезапустите службу Сервера администрирования.

В результате проверка уникальности имени будет выполнена на всех виртуальных Серверах и на главном Сервере администрирования.

Добавление группы безопасности

Вы можете добавлять группы безопасности (группы пользователей), гибко настраивать состав групп и доступ группы безопасности к разным функциям приложения. Группам безопасности можно давать названия, соответствующие их назначению. Например, название может соответствовать расположению пользователей в офисе или названию структурного подразделения компании, к которому относятся пользователи.

Один пользователь может входить в состав нескольких групп безопасности. Учетная запись пользователя под управлением виртуального Сервера администрирования может входить только в группы безопасности этого виртуального Сервера и иметь права доступа только в рамках этого виртуального Сервера.

Чтобы добавить группу безопасности:

1. В дереве консоли выберите папку **Учетные записи пользователей**.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. Нажмите на кнопку **Добавить группу безопасности**.

   Откроется окно **Добавить группу безопасности**.

3. В окне **Добавить группу безопасности** в разделе **Общие** укажите имя группы.

Имя группы не может превышать 255 символов и не может содержать символы *, <, >, ?, \, :, |. Имя группы должно быть уникальным.

Вы можете ввести описание группы в поле ввода **Описание**. Заполнение поля **Описание** не является обязательным.

4. Нажмите на кнопку **OK**.

Добавленная группа безопасности отобразится в папке **Учетные записи пользователей** в дереве консоли. Вы можете добавить пользователей в созданную группу.

Добавление пользователя в группу

Чтобы добавить пользователя в группу:

1. В дереве консоли выберите папку **Учетные записи пользователей**.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В списке учетных записей пользователей и групп выберите группу, в которую нужно добавить пользователя.

3. В окне свойств группы выберите раздел **Пользователи группы**, затем нажмите на кнопку **Добавить**.

   В результате откроется окно со списком пользователей.

4. В списке выберите пользователя или пользователей, которых нужно включить в состав группы.

5. Нажмите на кнопку **OK**.

Пользователь добавлен в группу и отображается в списке пользователей группы.

Настройка прав доступа к функциям приложения. Управление доступом на основе ролей

Kaspersky Security Center предоставляет доступ на основе ролей к функциям Kaspersky Security Center и к функциям управляемых приложений "Лаборатории Касперского".

Вы можете настроить права доступа к функциям приложения для пользователей Kaspersky Security Center 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.

Роль пользователя (далее также роль) – это заранее определенный набор прав доступа к функциям Kaspersky Security Center или управляемым приложениям "Лаборатории Касперского". Роль можно назначить пользователю или группе пользователей.

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 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.	Отсутст

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 Чтение ко всем объектам: **Чтение**.	Отсутствует.	Отсутствует.	Отсутст
Общие функции: Базовая функциональность	• **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с выборками устройств**	• Правила перемещения устройства (создание, изменение или удаление) для виртуального Сервера: **Запись**, **Выполнение операций с 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**. • Просмотр ключа восстановления для восстановления доступа к жесткому диску зашифрованному с помощью BitLocker: **Выполнение**.	• 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 об инцидентах. • Отчет о событиях. • Отчет о работе точек распространения. • Отчет о подчиненных Серверах администрирования. • Отчет о событиях Контроля устройств. • Отчет об уязвимостях. • Отчет о запрещенных приложениях. • Отчет о работе Веб-Контроля. • Отчет о статусе шифрования управляемых устройств. • Отчет о статусе шифрования запоминающих устройств. • Отчет об ошибках шифрования файлов. • Отчет о блокировании доступа к зашифрованным файлам. • Отчет о правах доступа к зашифрованным устройствам.	Отсутст

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
				• 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.	Отсутст
Общие функции: Обработка событий	• **Удалить события** • **Изменить параметры уведомлений о событиях** • **Изменить параметры регистрации событий** • **Запись**	• Изменение параметров регистрации событий: **Изменить параметры регистрации событий**. • Изменение параметров уведомления о событиях: **Изменить параметры уведомлений о событиях**. • Удаление событий: **Удалить события**.	Отсутствует.	Отсутствует.	Парамет • Пар вир кол обн вир нео соз вир • Пар вир пер оце обн вир • Мак кол соб хра баз • Пер соб уда уст
Общие функции: Операции с Сервером администрирования	• **Чтение** • **Запись** • **Выполнение** • **Изменение списков управления доступом объектов** • **Выполнение операций с выборками устройств**	• Изменение портов Сервера администрирования для подключения Агента администрирования: **Запись**. • Изменение портов прокси-сервера активации, запущенного на Сервере администрирования: **Запись**. • Изменение портов прокси-сервера активации для мобильных устройств, запускаемых на Сервере администрирования: **Запись**. • Изменение портов Веб-сервера для распространения автономных пакетов: **Запись**. • Изменение портов Веб-сервера для распространения iOS MDM-профилей: **Запись**.	• Резервное копирование данных Сервера администрирования. • Обслуживание базы данных.	Отсутствует.	Отсутст

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
		• Изменение SSL-портов Сервера администрирования для подключения с помощью Kaspersky Security Center Web Console: **Запись**. • Изменение портов Сервера администрирования для подключения мобильных устройств: **Запись**. • Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования: **Запись**. • Укажите максимальное количество событий, которое может отправлять Сервер администрирования: **Запись**. • Изменение периода, в течение которого Сервер администрирования может отправлять события: **Запись**.			
Общие функции: Развертывание приложений "Лаборатории Касперского"	• **Управление патчами "Лаборатории Касперского"** • **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с выборками устройств**	Одобрить или отклонить установку патча: **Управление патчами "Лаборатории Касперского"**.	Отсутствует.	• Отчет об использовании лицензионных ключей виртуальным Сервером администрирования. • Отчет о версиях приложений "Лаборатории Касперского". • Отчет о несовместимых приложениях. • Отчет о версиях обновлений модулей приложений "Лаборатории Касперского". • Отчет о развертывании защиты.	Инсталл пакет: "Г "Лаборат Касперс
Общие функции: Управление лицензионными ключами	• **Экспортировать файл ключа** • **Запись**	• Экспорт файл ключа: **Экспортировать файл ключа**. • Изменение параметров лицензионного ключа Сервера администрирования: **Запись**.	Отсутствует.	Отсутствует.	Отсутст
Общие функции: Управление отчетами	• **Чтение** • **Запись**	• Создание отчетов для объектов независимо от их	Отсутствует.	Отсутствует.	Отсутст

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
		списков ACL: **Запись**. • Выполнять отчеты независимо от их списков ACLs: **Чтение**.			

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Д
Общие функции: Иерархия Серверов администрирования	**Настроить иерархию Серверов администрирования**	Добавление, обновление или удаление подчиненных Серверов администрирования: **Настроить иерархию Серверов администрирования**.	Отсутствует.	Отсутствует.	Отсутст
Общие функции: Права пользователей	**Изменение списков управления доступом объектов**	• Изменение свойств Безопасности любого объекта: **Изменение списков управления доступом объектов**. • Управление ролями пользователей: **Изменение списков управления доступом объектов**. • Управление внутренними пользователями: **Изменение списков управления доступом объектов**. • Управление группами безопасности: **Изменение списков управления доступом объектов**. • Управление псевдонимами: **Изменение списков управления доступом объектов**.	Отсутствует.	Отсутствует.	Отсутст
Общие функции: Виртуальные Серверы администрирования	• **Управление виртуальными Серверами** • **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с 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**.	Отсутствует.	Отчет о результатах установки обновлений стороннего ПО.	Отсутст

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Д
		• Перемещение виртуального Сервера администрирования в другую группу: **Управление виртуальными Серверами**. • Установка прав доступа к виртуальному Серверу администрирования: **Управление виртуальными Серверами**.			
Общие функции: Управление ключами шифрования	• **Чтение** • **Запись**	• Экспорт ключей шифрования: **Чтение**. • Импорт ключей шифрования: **Запись**.	Отсутствует.	Отсутствует.	Отсутст
Управление мобильными устройствами: Основные	• **Подключение новых устройств** • **Отправка только информационных команд на мобильные устройства** • **Отправка команд на мобильные устройства** • **Управление сертификатами** • **Чтение** • **Запись**	• Получение восстановленных данных службы управления ключами: **Чтение**. • Удаление сертификатов пользователей: **Управление сертификатами**. • Получение публичной части сертификата пользователя: **Чтение**. • Проверка, включена ли инфраструктура открытых ключей: **Чтение**. • Проверка учетной записи инфраструктуры открытых ключей: **Чтение**. • Получение шаблонов инфраструктуры открытых ключей: **Чтение**. • Получение шаблонов инфраструктуры открытых ключей с помощью расширенного использования ключа (EKU) сертификата: **Чтение**. • Проверка, не отозван ли сертификат инфраструктуры открытых ключей: **Чтение**. • Обновление параметров выпуска сертификатов пользователя: **Управление сертификатами**.	Отсутствует.	Отсутствует.	Отсутст

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
		• Получение параметров выпуска сертификатов пользователя: **Чтение**. • Получение пакетов по названию и версиям приложений: **Чтение**. • Установка или отмена сертификатов пользователя: **Управление сертификатами**. • Обновление сертификата пользователя: **Управление сертификатами**. • Установка тега для сертификата пользователя: **Управление сертификатами**. • Запуск генерации инсталляционного пакета, содержащего iOS MDM-профиль; отмена генерации инсталляционного пакета, содержащего iOS MDM-профиль: **Подключение новых устройств**.			
Управление системой: Подключения	• **Запуск RDP-сессий** • **Подключение к существующим RDP-сессиям** • **Создание туннелирования** • **Сохранение файлов с устройств на рабочем месте администратора** • **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с выборками устройств**	• Создание сеанса совместного доступа к рабочему столу: **Запуск RDP-сессий**. • Создание RDP-сеанса: **Подключение к существующим RDP-сессиям**. • Создание туннеля: **Создание туннелирования**. • Сохранение списка сетей: **Сохранение файлов с устройств на рабочем месте администратора**.	Отсутствует.	Отчет о пользователях устройства.	Отсутст
Управление системой: Инвентаризация оборудования	• **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с выборками устройств**	• Получение или экспорт объектов инвентаризации оборудования: **Чтение**. • Добавление, настройка или удаление объектов инвентаризации оборудования: **Запись**.	Отсутствует.	• Отчет о реестре оборудования. • Отчет об изменении конфигурации. • Отчет об оборудовании.	Отсутст
Управление системой: Network Access Control	• **Чтение** • **Запись**	• Просмотр параметров Cisco: **Чтение**. • Изменение	Отсутствует.	Отсутствует.	Отсутст

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Д
		параметров Cisco: **Запись**.			
Управление системой: Развертывание операционной системы	• **Развертывание PXE-серверов** • **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с 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.	Инсталл пакет: О операци системы
Управление системой: Системное администрирование	• **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с 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. • Закрытие уязвимостей. • Установка требуемых обновлений и закрытия уязвимостей.	Отчет об обновлениях ПО.	Отсутст
Управление системой: Удаленная установка	• **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с выборками устройств**	• Просмотр Системного администрирования стороннего производителя на основе свойств инсталляционного пакета: **Чтение**. • Изменение Системного администрирования на основе свойств инсталляционного пакета: **Запись**.	Отсутствует.	Отсутствует.	Инсталл пакеты: • Пол при • Паке
Управление системой: Инвентаризация приложений	• **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с 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.	Отсутст

Предопределенные роли пользователей

Роли пользователей, назначенные пользователям Kaspersky Security Center, предоставляют им набор прав доступа к функциям приложения.

Пользователям, которые были созданы на виртуальном Сервере, невозможно назначить роли на Сервере администрирования.

Вы можете использовать предопределенные роли пользователей с уже настроенным набором прав или создавать роли. При создании роли вам нужно задать область действия и назначить права доступа к функциям Kaspersky Security Center. Некоторые из предопределенных ролей пользователей, доступных в Kaspersky Security Center, могут быть связаны с определенными должностями, например, **Аудитор**, **Специалист по безопасности**, **Контролер** (эти роли присутствуют в Kaspersky Security Center 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**.

Роль	Описание

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 функциональной области **Общие функции**: • **Доступ к объектам независимо от их списков ACL.** • **Удаленные объекты.** • **Управление отчетами.** Вы можете назначить эту роль сотруднику, который выполняет аудит вашей организации.

Администратор установки приложений	Разрешает все операции в следующих функциональных областях:
	• **Общие функции**:
	  • **Базовая функциональность.**
	  • **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 области **Общие функции: Базовая функциональность**.

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**.

Роль	Описание
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**.

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.
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**: функциональная область **Управление отчетами**. Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации.
Администратор Системного администрирования	Разрешает все операции в области **Общие функции**: **Базовая функциональность** и **Управление системой** (включая все функции).
Оператор Системного администрирования	Предоставляет права на **Чтение** и **Выполнение** (если применимо) в области **Общие функции**: **Базовая функциональность** и **Управление системой** (включая все функции).

Добавление роли пользователя

Чтобы добавить роль пользователя:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойства Сервера администрирования в панели **Разделы** перейдите в раздел **Роли пользователей** и нажмите на кнопку **Добавить**.

   Раздел **Роли пользователей** доступен, если включен параметр **Отображать разделы с параметрами безопасности**.

4. В окне **Новая роль** настройте параметры роли:

   - В панели **Разделы** выберите раздел **Общие** и укажите имя роли.

     Имя роли не может превышать 100 символов.

   - В разделе **Права** настройте набор прав, установив флажки **Разрешить** и **Запретить** напротив функций приложения.

   Если вы работаете на главном Сервере администрирования, вы можете включить параметр **Передать список ролей подчиненному Серверу администрирования**.

5. Нажмите на кнопку **OK**.

Роль добавлена.

Роли пользователей, созданные для Сервера администрирования, отображаются в окне свойств Сервера в разделе **Роли пользователей**. Вы можете изменять и удалять роли пользователей, а также назначать роли группам безопасности или отдельным пользователям.

Назначение роли пользователю или группе безопасности

Чтобы назначить роль пользователю или группе пользователей:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Безопасность**.

   Раздел **Безопасность** доступен, если в окне параметров интерфейса установлен флажок **Отображать разделы с параметрами безопасности**.

4. В поле **Имена групп или пользователей** выберите пользователя или группу пользователей, которой нужно присвоить роль.

   Если пользователь или группа отсутствует в поле, добавьте их по кнопке **Добавить**.

При добавлении пользователя по кнопке **Добавить** можно выбрать тип аутентификации пользователя (Microsoft Windows или Kaspersky Security Center). Аутентификация Kaspersky Security Center используется для выбора учетных записей внутренних пользователей, которые используются для работы с виртуальными Серверами администрирования.

5. Перейдите на вкладку **Роли** и нажмите на кнопку **Добавить**.

   Откроется окно **Роли пользователей**. В окне отображаются созданные роли пользователей.

6. В окне **Роли пользователей** выберите роль для группы безопасности.

7. Нажмите на кнопку **ОК**.

В результате роль с набором прав на работу с Сервером администрирования будет назначена пользователю или группе безопасности. Назначенные роли отображаются на вкладке **Роли** в разделе **Безопасность** окна свойств Сервера администрирования.

Назначение прав пользователям или группам пользователей

Вы можете назначить права пользователям или группам пользователей, чтобы использовать различные возможности Сервера администрирования и приложений "Лаборатории Касперского", для которых у вас есть плагины управления, например, Kaspersky Endpoint Security для Windows.

Чтобы назначить права пользователю или группе пользователей:

1. В дереве консоли выполните одно из следующих действий:

   - Раскройте узел **Сервер администрирования** и выберите подпапку с именем требуемого Сервера администрирования.
   - Выберите группу администрирования.

2. В контекстном меню Сервера администрирования или группы администрирования выберите пункт **Свойства**.

3. В открывшемся окне свойств Сервера администрирования (или окне свойств группы администрирования) в панели **Разделы** выберите раздел **Безопасность**.

   Раздел **Безопасность** доступен, если в окне параметров интерфейса установлен флажок **Отображать разделы с параметрами безопасности**.

4. В разделе **Безопасность** в списке **Имена групп или пользователей** выберите пользователя или группу пользователей.

5. В списке прав в нижней части окна, на вкладке **Права** настройте права для пользователей или групп:

   a. Нажмите на значок плюс (+), чтобы раскрыть узел в списке, и назначьте права.

   b. Установите флажки **Разрешить** и **Запретить** рядом с требуемыми правами.

      Пример 1: Раскройте узел **Доступ к объектам независимо от их списков ACL** или узел **Удаленные объекты** и выберите **Чтение**.

Пример 2: Раскройте узел **Базовая функциональность** и выберите **Запись**.

6. После того как вы настроили набор прав, нажмите на кнопку **Применить**.

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.
  - Обработка событий.
  - Операции с Сервером администрирования (только в окне свойств Сервера администрирования).
  - Развертывание приложений "Лаборатории Касперского".
  - Управление лицензионными ключами.
  - Управление отчетами.
  - Иерархия Серверов.
  - Права пользователей.
  - Виртуальные Серверы администрирования.
- Управление мобильными устройствами:
  - Общие.
- Управление системой:
  - Подключения.
  - Инвентаризация оборудования.
  - Управление доступом в сеть.
  - Развертывание операционной системы.
  - Управление уязвимостями и патчами.
  - 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.

Распространение пользовательских ролей на подчиненные Серверы администрирования

По умолчанию списки пользовательских ролей главного и подчиненного Серверов администрирования являются независимыми. Вы можете настроить приложения для автоматического распространения ролей пользователей, созданных на главном Сервере администрирования, на все подчиненные Сервера администрирования. Роли пользователей также могут распространяться с подчиненного Сервера администрирования на собственные подчиненные Сервера администрирования.

Чтобы распространить роли пользователей с главного Сервера администрирования на подчиненные Серверы администрирования:

1. Откройте главное окно приложения.
2. Выполните одно из следующих действий:
   - В дереве консоли в контекстном меню требуемого Сервера администрирования выберите пункт **Свойства**.
   - Если у вас есть активная политика Сервера администрирования, в рабочей области папки **Политики** в контекстном меню этой политики выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования или в окне свойств политики в панели **Разделы** перейдите в раздел **Роли пользователей**.

   Раздел **Роли пользователей** доступен, если включен параметр **Отображать разделы с параметрами безопасности**.

4. Включите параметр **Передать список ролей подчиненному Серверу администрирования**.
5. Нажмите на кнопку **ОК**.

Приложение копирует роли пользователей главного Сервера администрирования на подчиненные Серверы администрирования.

Если параметр **Передать список ролей подчиненному Серверу администрирования** включен и роли пользователей распространены, такие роли не доступны для изменений или удаления на подчиненном Сервере администрирования. Когда вы создаете роль или изменяете существующую роль на главном Сервере администрирования, изменения автоматически копируются на подчиненные Серверы администрирования. Когда вы удаляете роль пользователя на главном Сервере администрирования, эта роль остается на подчиненном Сервере администрирования и может быть изменена или удалена.

Роли, которые распространяются на подчиненный Сервер администрирования с главного Сервера, отображаются с помощью значка замка (🔒). Вы не можете изменять эти роли на подчиненном Сервере администрирования.

Если роль создается на главном Сервере администрирования, а на подчиненном Сервере администрирования есть роль с таким же именем, новая роль копируется на подчиненный Сервер администрирования, и к ее имени в скобках добавляется номер, например, ~~1, ~~2 (номер может быть случайным).

Если выключить параметр **Передать список ролей подчиненному Серверу администрирования**, все роли пользователя останутся на подчиненных Серверах администрирования, но станут независимыми от ролей на главном Сервере администрирования. Когда роли на подчиненных Серверах администрирования становятся независимыми, их можно изменять или удалять.

Назначение пользователя владельцем устройства

Вы можете назначить пользователя владельцем устройства, чтобы "закрепить" устройство за этим пользователем. При необходимости выполнить какие-либо действия с устройством (например, обновить аппаратное обеспечение) администратор может проинформировать владельца устройства и согласовать действия с ним.

Чтобы назначить пользователя владельцем устройства:

1. В дереве консоли выберите папку **Управляемые устройства**.
2. В рабочей области папки на вкладке **Устройства** выберите устройство, для которого нужно назначить владельца.
3. В контекстном меню устройства выберите пункт **Свойства**.
4. В окне свойств устройства выберите **Информация о системе** → **Сеансы**.
5. Нажмите на кнопку **Назначить** рядом с полем **Владелец устройства**.
6. В окне **Выбор пользователя** выберите пользователя, которого нужно назначить владельцем устройства и нажмите на кнопку **OK**.
7. Нажмите на кнопку **OK**.

В результате владелец устройства будет назначен. По умолчанию поле **Владелец устройства** заполнено значением из Active Directory и обновляется при каждом опросе Active Directory. Вы можете просмотреть список владельцев устройств в отчете **Отчет о владельцах устройств**. Отчет можно создать с помощью мастера создания отчетов.

Рассылка сообщений пользователям

Чтобы отправить сообщение пользователю по электронной почте:

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню пользователя выберите **Уведомлять по электронной почте**.

3. Заполните необходимые поля в окне **Сообщение для пользователя** и нажмите на кнопку **OK**.

В результате сообщение будет отправлено на электронную почту, указанную в свойствах пользователя.

Чтобы отправить SMS-сообщение пользователю:

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.

2. В контекстном меню пользователя выберите **Отправить SMS-сообщение**.

3. Заполните необходимые поля в окне **Текст SMS** и нажмите на кнопку **OK**.

В результате сообщение будет отправлено на мобильное устройство, номер которого указан в свойствах пользователя.

Просмотр списка мобильных устройств пользователя

Чтобы просмотреть список мобильных устройств пользователя:

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню учетной записи пользователя выберите пункт **Свойства**.

3. В окне свойств учетной записи пользователя выберите раздел **Мобильные устройства**.

В разделе **Мобильные устройства** можно просмотреть список мобильных устройств пользователя и информацию о мобильных устройствах. По кнопке **Экспортировать в файл** можно сохранить список мобильных устройств в файле.

Установка сертификата пользователю

Вы можете установить пользователю сертификаты трех типов:

- общий сертификат, необходим для идентификации мобильного устройства пользователя;
- почтовый сертификат, необходим для настройки корпоративной почты на мобильном устройстве пользователя;
- VPN-сертификат, необходим для настройки виртуальной частной сети на мобильном устройстве пользователя.

Чтобы выписать пользовательский сертификат и установить его:

1. В дереве консоли откройте папку **Учетные записи пользователей** и выберите учетную запись пользователя.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню учетной записи пользователя выберите пункт **Установить сертификат**.

Будет запущен мастер установки сертификата. Следуйте далее указаниям мастера.

В результате работы мастера установки сертификата сертификат будет создан и установлен пользователю. Список установленных сертификатов пользователя можно просмотреть и экспортировать в файл.

Просмотр списка сертификатов, выписанных пользователю

Чтобы просмотреть список всех сертификатов, выписанных пользователю:

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню учетной записи пользователя выберите пункт **Свойства**.

3. В окне свойств учетной записи пользователя выберите раздел **Сертификаты**.

В разделе **Сертификаты** можно просмотреть список сертификатов пользователя и информацию о сертификатах. По кнопке **Экспортировать в файл** можно сохранить список сертификатов в файле.

Об администраторе виртуального Сервера администрирования

Администратор сети организации, находящейся под управлением виртуального Сервера, будет запускать Kaspersky Security Center Web Console для просмотра сведений о состоянии антивирусной защиты сети под именем учетной записи, указанной в этом окне.

При необходимости можно создать несколько учетных записей администраторов виртуального Сервера.

Пользователям, которые были созданы на виртуальном Сервере, невозможно назначить роли на Сервере администрирования.

Администратор виртуального Сервера администрирования является внутренним пользователем Kaspersky Security Center. Сведения о внутренних пользователях не передаются операционной системе. Аутентификацию внутренних пользователей осуществляет Kaspersky Security Center.

Удаленная установка операционных систем и приложений

Kaspersky Security Center позволяет централизованно создавать образы операционных систем и разворачивать их на клиентских устройствах по сети, а также выполнять удаленную установку приложений "Лаборатории Касперского" или других производителей программного обеспечения.

Для создания образов операционных систем установите Windows ADK и средства дополнения Windows PE для Windows ADK на Сервере администрирования. Вы можете создать образ любой версии операционной системы Windows, отвечающей требованиям Kaspersky Security Center.

Kaspersky Security Center не поддерживает 64-разрядные версии Windows ADK и Windows PE.

Захват образов операционных систем

Kaspersky Security Center может выполнять захват образов операционных систем устройств и доставлять эти образы на Сервер администрирования. Такие образы операционных систем хранятся на Сервере администрирования в специальной папке. Снятие и создание образа операционной системы эталонного устройства выполняется с помощью задачи создания инсталляционного пакета.

Функциональность захвата образа операционной системы имеет следующие особенности:

- Образ операционной системы невозможно снимать с устройства, на котором установлен Сервер администрирования.
- Во время снятия образа операционной системы происходит обнуление параметров эталонного устройства утилитой sysprep.exe. В случае необходимости восстановления параметров эталонного устройства в мастере создания задачи снятия образа ОС необходимо установить флажок **Сохранять резервную копию состояния устройства**.
- В процессе снятия образа выполняется перезагрузка эталонного устройства.

Развертывание образов операционных систем на новых устройствах

Вы можете использовать полученные образы для развертывания на новых устройствах в сети, на которых еще не была установлена операционная система. Для этой цели используется технология Preboot eXecution Environment (PXE). Вы назначаете устройство в сети, которое будет использоваться в качестве PXE-сервера. Это устройство должно отвечать следующим требованиям:

- на устройстве должен быть установлен Агент администрирования;
- на устройстве не должен работать DHCP-сервер, так как PXE-сервер использует те же порты, что и DHCP;
- в сегменте сети, в который входит устройство, не должно быть других PXE-серверов.

Для развертывания операционной системы должны быть выполнены следующие условия:

- на устройстве должна быть установлена сетевая карта;
- устройство должно быть подключено к сети;
- при загрузке устройства в BIOS необходимо выбрать параметр загрузки по сети.

Развертывание операционной системы выполняется в следующей последовательности:

1. Клиентское устройство устанавливает соединение с PXE-сервером при загрузке клиентского устройства.
2. Клиентское устройство загружается в среде Windows Preinstallation Environment (WinPE).

   Для включения устройства в среду WinPE может потребоваться настройка состава драйверов для среды WinPE.

3. Клиентское устройство регистрируется на Сервере администрирования.
4. Администратор назначает клиентскому устройству инсталляционный пакет с образом операционной системы.

   Администратор может добавлять необходимые драйверы в инсталляционный пакет с образом операционной системы. Администратор также может указывать конфигурационный файл с параметрами операционной системы (файл ответов), которые должны применяться во время установки.

5. Выполняется развертывание операционной системы на клиентском устройстве.

Администратор может вручную указать MAC-адреса еще не подключившихся клиентских устройств и назначить им инсталляционный пакет с образом операционной системы. Когда указанные клиентские устройства подключаются к PXE-серверу, автоматически выполняется установка операционной системы на этих устройствах.

Развертывание образов операционных систем на устройствах с уже установленной операционной системой

Развертывание образов операционной системы на клиентских устройствах, на которых уже установлена рабочая операционная система, выполняется с помощью задачи удаленной установки для наборов устройств.

Обратите внимание, что выполняется чистая установка операционной системы. Все данные будут удалены.

Установка приложений "Лаборатории Касперского" и других производителей программного обеспечения

Администратор может создавать инсталляционные пакеты любых приложений, включая приложения, указанные пользователем, и устанавливать эти приложения на клиентские устройства с помощью задачи удаленной установки.

Создание образов операционных систем

Создание образов операционных систем выполняется при помощи задачи снятия образа операционной системы эталонного устройства.

Чтобы создать задачу снятия образа операционной системы:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. По кнопке **Создать инсталляционный пакет** запустите мастер создания инсталляционного пакета.
3. В окне мастера **Выбор типа инсталляционного пакета** нажмите на кнопку **Создать инсталляционный пакет с образом операционной системы**.
4. Следуйте далее указаниям мастера.

   В результате работы мастера создается задача Сервера администрирования **Создание инсталляционного пакета на основе образа ОС эталонного устройства**. Задачу можно просмотреть в папке **Задачи**.

В результате выполнения задачи **Создание инсталляционного пакета на основе образа ОС эталонного устройства** создается инсталляционный пакет, который можно использовать для развертывания операционной системы на клиентских устройствах с помощью PXE-сервера или задачи удаленной установки. Просмотреть инсталляционный пакет можно в папке **Инсталляционные пакеты**.

Установка образов операционных систем

Kaspersky Security Center позволяет разворачивать на устройства сети организации wim-образы настольных и серверных версий операционных систем Windows.

Образ операционной системы, пригодный для развертывания средствами Kaspersky Security Center, может быть получен следующими способами:

- импортом из файла install.wim, который входит в состав дистрибутива Windows;
- захватом образа с эталонного устройства.

Поддерживаются два сценария развертывания образа операционной системы:

- развертывание на "чистое" устройство, то есть на устройство без установленной на нем операционной системы;
- развертывание на устройство, работающее под управлением операционной системы Windows.

Используйте Use Windows Preinstallation Environment (Windows PE) для захвата и развертывания образов операционной системы. В WinPE следует добавить все драйверы, необходимые для правильной работы всех устройств. Как правило, необходимо добавить драйверы сетевого адаптера и контроллера устройства хранения.

Для реализации сценариев развертывания и захвата образов должны быть выполнены следующие требования:

- На Сервер администрирования должен быть установлен Windows Automated Installation Kit (WAIK) версии 2.0 и выше или Windows ADK с надстройкой Windows PE для Windows ADK. Если предполагаются работы по установке или захвату образов на Windows XP, следует установить WAIK.
- В сети, в которой расположено устройство, должен присутствовать DHCP-сервер.
- Папка общего доступа Сервера администрирования должна быть доступна для чтения из сети, в которой находится устройство. Если папка общего доступа расположена на Сервере администрирования, то доступ нужен для учетной записи KlPxeUser (эта учетная запись создается автоматически на этапе работы инсталлятора Сервера администрирования). Если папка расположена вне Сервера администрирования, то доступ нужен для всех.

При выборе образа операционной системы для установки администратор должен явно указать архитектуру процессора устройства: x86 или x86-64.

Настройка адреса прокси-сервера KSN

По умолчанию название соединения или IP-адрес Сервера администрирования совпадает с адресом прокси-сервера KSN. При изменении названия соединения или IP-адреса для Сервера администрирования необходимо указать правильный адрес прокси-сервера KSN, чтобы предотвратить потерю связи между устройствами и KSN.

Чтобы настроить адреса прокси-сервера KSN:

1. В дереве консоли перейдите в раздел **Дополнительно → Удаленная установка → Инсталляционные пакеты**.
2. В контекстном меню папки **Инсталляционные пакеты** выберите пункт **Свойства**.
3. В открывшемся окне укажите новый адрес прокси-сервера KSN на вкладке **Общие**.
4. Нажмите на кнопку **Применить**.

С этого момента указанный адрес используется как адрес прокси-сервера KSN. Рекомендуется включить параметр **Использовать прокси-сервер KSN** для оптимизации трафика в сети.

Добавление драйверов для среды предустановки Windows (WinPE)

Чтобы добавить драйверы для среды предустановки Windows (WinPE):

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Развертывание образов устройств**.
2. В рабочей области папки **Развертывание образов устройств** нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Настроить состав драйверов для среды предустановки Windows (WinPE)**.

   Откроется окно **Драйверы для среды предустановки Windows**.
3. В окне **Драйверы для среды предустановки Windows** нажмите на кнопку **Добавить**.

   Откроется окно **Выбор драйвера**.
4. В окне **Выбор драйвера** выберите драйвер из списка.

   Если необходимый драйвер отсутствует в списке, нажмите на кнопку **Добавить** и в открывшемся окне **Добавление драйвера** укажите имя драйвера и папку дистрибутива драйвера.

   Вы можете выбрать папку по кнопке **Обзор**.

   В окне **Добавление драйвера** нажмите на кнопку **OK**.
5. В окне **Выбор драйвера** нажмите на кнопку **OK**.

   Драйвер будет добавлен в хранилище Сервера администрирования. Добавленный в хранилище драйвер отображается в окне **Выбор драйвера**.
6. В окне **Драйверы для среды предустановки Windows** нажмите на кнопку **OK**.

Драйвер будет добавлен в среду предустановки Windows (WinPE).

Добавление драйверов в инсталляционный пакет с образом операционной системы

Чтобы добавить драйверы в инсталляционный пакет с образом операционной системы:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета с образом операционной системы выберите пункт **Свойства**.

   Откроется окно свойств инсталляционного пакета.
3. В окне свойств инсталляционного пакета выберите раздел **Дополнительные драйверы**.
4. Нажмите на кнопку **Добавить**, расположенную в разделе **Дополнительные драйверы**.

   Откроется окно **Выбор драйвера**.

5. В окне **Выбор драйвера** выберите драйверы, которые вы хотите добавить в инсталляционный пакет с образом операционной системы.

   Новые драйверы можно добавить в хранилище Сервера администрирования при нажатии на кнопку **Добавить** в окне **Выбор драйвера**.

6. Нажмите на кнопку **OK**.

Добавленные драйверы отображаются в разделе **Дополнительные драйверы** в окне свойств инсталляционного пакета с образом операционной системы.

Настройка параметров утилиты sysprep.exe

Утилита sysrep.exe используется для подготовки устройства к созданию с него образа операционной системы.

Чтобы настроить параметры утилиты sysprep.exe:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.

2. В контекстном меню инсталляционного пакета с образом операционной системы выберите пункт **Свойства**.

   Откроется окно свойств инсталляционного пакета.

3. В окне свойств инсталляционного пакета выберите раздел **Параметры sysprep.exe**.

4. В разделе **Параметры sysprep.exe** укажите конфигурационный файл, который будет использоваться при развертывании операционной системы на клиентском устройстве:

   - **Использовать конфигурационный файл по умолчанию**. Выберите этот вариант, чтобы использовать файл ответов, создаваемый по умолчанию во время снятия образа операционной системы.

   - **Задать пользовательские значения основных параметров**. Выберите этот вариант, чтобы задать значения параметров с помощью пользовательского интерфейса.

   - **Задать конфигурационный файл**. Выберите этот вариант, чтобы использовать собственный файл ответов.

5. Нажмите на кнопку **Применить**, чтобы внесенные изменения вступили в силу.

Развертывание операционных систем на новых устройствах в сети

Чтобы развернуть операционную систему на новых устройствах, на которых еще не установлена операционная система:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Развертывание образов устройств**.

   Убедитесь, что в окне **Настройка интерфейса** включен параметр **Отображать Системное администрирование**. Иначе папка **Удаленная установка** не отображается.

2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите значение **Управлять списком PXE-серверов в сети**.

   Откроется окно **Свойства**: **Развертывание образов устройств** на разделе **PXE-серверы**.

3. В разделе **PXE-серверы** нажмите на кнопку **Добавить** и в открывшемся окне **PXE-серверы** выберите устройство, которое будет использоваться как PXE-сервер.

   Добавленное устройство отобразится в разделе PXE-серверы. Созданные WinPE-файлы передаются на устройство с Сервера администрирования. Процесс передачи файлов обычно занимает 10 минут. После завершения передачи файлов отображаемое значение **Статус** меняется с **Начало работы** на **Готов**.

4. В разделе **PXE-серверы** выберите PXE-сервер и нажмите на кнопку **Свойства**.

5. В окне свойств выбранного PXE-сервера в разделе **Параметры подключения к PXE-серверу** выполните настройку параметров подключения Сервера администрирования к PXE-серверу.

6. Выполните загрузку клиентского устройства, на котором вы хотите развернуть операционную систему.

7. В среде BIOS клиентского устройства выберите вариант установки Network boot.

   Клиентское устройство подключается к PXE-серверу и отображается в рабочей области папки **Развертывание образов устройств**.

8. В блоке **Действия** по ссылке **Назначить инсталляционный пакет** выберите инсталляционный пакет, который будет использоваться для установки операционной системы на выбранное устройство.

   Используйте инструмент DiskPart на выбранном устройстве, чтобы проверить доступные диски. В командной строке Windows PE введите `diskpart`, чтобы открыть инструмент DiskPart. Введите `list disk`, чтобы просмотреть список дисков.

   После добавления устройства и назначения для него инсталляционного пакета развертывание операционной системы на этом устройстве начинается автоматически.

9. Для отмены развертывания операционной системы на клиентском устройстве воспользуйтесь ссылкой **Отменить установку образов ОС** в блоке **Действия**.

Чтобы добавить устройства по MAC-адресу, выполните одно из следующих действий:

- по ссылке **Добавить MAC-адрес устройства** в папке **Развертывание образов устройств** откройте окно **Новое устройство** и укажите MAC-адрес устройства, которое вы хотите добавить;

- по ссылке **Импортировать MAC-адреса устройств из файла** в папке **Развертывание образов устройств** выберите файл, содержащий список MAC-адресов всех устройств, на которых вы хотите развернуть операционную систему.

Развертывание операционных систем на клиентских устройствах

Чтобы выполнить развертывание операционной системы на клиентских устройствах с уже установленной операционной системой:

1. В дереве консоли откройте папку **Удаленная установка** и перейдите по ссылке **Развернуть инсталляционный пакет на управляемые устройства (рабочие места)**, чтобы запустить мастер развертывания защиты.

2. В окне мастера **Выбор инсталляционного пакета** укажите инсталляционный пакет с образом операционной системы.

3. Следуйте далее указаниям мастера.

В результате работы мастера создается задача удаленной установки операционной системы на клиентских устройствах. Запустить или остановить задачу можно в папке **Задачи**.

Создание инсталляционных пакетов приложений

Чтобы создать инсталляционный пакет приложения:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.

2. По кнопке **Создать инсталляционный пакет** запустите мастер создания инсталляционного пакета.

3. В окне мастера **Выбор типа инсталляционного пакета** нажмите на одну из кнопок:

   - **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**. Выберите этот вариант, если вы хотите создать инсталляционный пакет для приложения "Лаборатории Касперского".

   - **Создать инсталляционный пакет для указанного исполняемого файла**. Выберите этот вариант, если вы хотите создать инсталляционный пакет для приложения с помощью исполняемого файла. Как правило, исполняемый файл является установочным файлом приложения.

     - **Копировать всю папку в инсталляционный пакет**

       Выберите этот параметр, если исполняемый файл сопровождается дополнительными файлами, необходимыми для установки приложения. Прежде чем включить этот параметр, убедитесь, что все требуемые файлы хранятся в одной папке. Если этот параметр включен, приложение добавляет все содержимое папки, включая указанный исполняемый файл, в инсталляционный пакет.

     - **Указать параметры установки**

       Чтобы удаленная установка прошла успешно, большинство приложений требуют, чтобы установка проводилась в тихом режиме. В этом случае вам нужно указать параметры автоматической установки.

       Настройте параметры установки:

       - **Параметры запуска исполняемого файла**

         Если приложению требуются дополнительные параметры для установки без вывода сообщений, укажите их в этом поле. Дополнительную информацию см. в документации производителя.

Вы также можете указать и другие параметры.

- **Конвертировать параметры на рекомендуемые значения для приложений, распознаваемых Kaspersky Security Center**

  Приложение будет установлено с рекомендуемыми параметрами, если информация об указанном приложении содержится в базе данных "Лаборатории Касперского".

  Если вы ввели параметры в поле **Параметры запуска исполняемого файла**, они будут изменены на рекомендуемые параметры.

  По умолчанию параметр включен.

  База данных "Лаборатории Касперского" создана и поддерживается аналитиками "Лаборатории Касперского". Для каждого приложения, добавляемого в базу данных, аналитики "Лаборатории Касперского" определяют оптимальные параметры установки. Параметры определяются так, чтобы обеспечить успешную удаленную установку приложения на клиентское устройство. База данных обновляется автоматически при запуске задачи Загрузка обновлений в хранилище Сервера администрирования.

- **Выбрать приложение из базы "Лаборатории Касперского" для создания инсталляционного пакета**. Выберите этот вариант, если вы хотите выбрать приложение стороннего производителя из базы "Лаборатории Касперского", для которого требуется создать инсталляционный пакет. База данных создается автоматически при запуске задачи Загрузка обновлений в хранилище Сервера администрирования; приложения отображаются в списке.

- **Создать инсталляционный пакет с образом операционной системы**. Выберите этот вариант, если вы хотите создать инсталляционный пакет с образом операционной системы эталонного устройства.

  В результате работы мастера создается задача Сервера администрирования с именем **Создание инсталляционного пакета на основе образа ОС эталонного устройства**. В результате выполнения этой задачи создается инсталляционный пакет, который можно использовать для развертывания образа операционной системы с помощью PXE-сервера или задачи удаленной установки.

4. Следуйте далее указаниям мастера.

В результате работы мастера создается инсталляционный пакет, который можно использовать для установки приложения на клиентские устройства. Вы можете просмотреть инсталляционный пакет в папке **Инсталляционные пакеты** дерева консоли.

Выписка сертификата для инсталляционных пакетов приложений

Чтобы выписать сертификат для инсталляционного пакета приложения:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.

   Папка **Удаленная установка** по умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню папки **Инсталляционные пакеты** выберите пункт **Дополнительно**.

   В результате откроется окно свойств папки **Инсталляционные пакеты**.

3. В окне свойств папки **Инсталляционные пакеты** выберите раздел **Подпись автономных пакетов**.

4. В разделе **Подпись автономных пакетов** нажмите на кнопку **Задать**.

   Откроется окно **Сертификат**.

5. В поле **Тип сертификата** выберите открытый или закрытый тип сертификата:

   - Если выбрано значение **Контейнер PKCS#12**, укажите файл сертификата и пароль.
   - Если выбрано значение **X.509-сертификат**:

     a. укажите файл закрытого ключа (файл с расширением prk или pem);

     b. укажите пароль закрытого ключа;

     c. укажите файл открытого ключа (файл с расширением cer).

6. Нажмите на кнопку **OK**.

В результате будет выписан сертификат для инсталляционного пакета приложения.

Установка приложений на клиентские устройства.

Чтобы установить приложение на клиентские устройства:

1. В дереве консоли откройте папку **Удаленная установка** и перейдите по ссылке **Развернуть инсталляционный пакет на управляемые устройства (рабочие места)**, чтобы запустить мастер развертывания защиты.
2. В окне мастера **Выбор инсталляционного пакета** укажите инсталляционный пакет приложения, которое вы хотите установить.
3. Следуйте далее указаниям мастера.

В результате работы мастера создается задача удаленной установки приложения на клиентских устройствах. Запустить или остановить задачу можно в папке **Задачи**.

Вы можете устанавливать Агент администрирования на клиентские устройства с операционными системами Windows, Linux и macOS с помощью мастера развертывания защиты.

Чтобы управлять 64-разрядными приложениями безопасности с помощью Kaspersky Security Center на устройствах с операционными системами Linux, необходимо использовать 64-разрядный Агент администрирования для Linux. Требуемую версию Агента администрирования можно загрузить с веб-сайта Службы технической поддержки.

Перед выполнением удаленной установки Агента администрирования на устройство с операционной системой Linux необходимо подготовить устройство.

Работа с ревизиями объектов

Этот раздел содержит информацию о работе с ревизиями объектов. Kaspersky Security Center позволяет отслеживать изменения объектов. Каждый раз, когда вы сохраняете изменения объекта, создается *ревизия.* Каждая ревизия имеет номер.

Объекты приложения, 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:

- сравнивать выбранную ревизию с текущей ревизией;
- сравнивать выбранные ревизии;
- сравнивать объект с выбранной ревизией другого однотипного объекта;
- просматривать выбранную ревизию;
- откатывать изменения объекта к выбранной ревизии;
- сохранять ревизии в файле формата TXT.

В окне свойств объектов, которые поддерживают работу с ревизиями, в разделе **История ревизий** отображается список ревизий объекта со следующей информацией:

- номер ревизии объекта;
- дата и время изменения объекта;
- имя пользователя, изменившего объект;
- выполненное действие с объектом;
- описание ревизии изменения параметров объекта.

О ревизиях объектов

Вы можете выполнять с ревизиями объектов следующие действия:

- сравнивать выбранную ревизию с текущей ревизией;
- сравнивать выбранные ревизии;
- сравнивать объект с выбранной ревизией другого однотипного объекта;
- просматривать выбранную ревизию;
- откатывать изменения объекта к выбранной ревизии;
- сохранять ревизии в файле формата TXT.

В окне свойств объектов, которые поддерживают работу с ревизиями, в разделе **История ревизий** отображается список ревизий объекта со следующей информацией:

- номер ревизии объекта;
- дата и время изменения объекта;
- имя пользователя, изменившего объект;
- выполненное действие с объектом;
- описание ревизии изменения параметров объекта.

Просмотр раздела История ревизий

Вы можете сравнить ревизии объекта с текущей ревизией, сравнить ревизии, выбранные в списке, или сравнить ревизию объекта с ревизией другого однотипного объекта.

*Чтобы просмотреть раздел **История ревизий** объекта:*

1. В дереве консоли выберите один из объектов:
   - узел **Сервер администрирования**;
   - папку **Политики**;
   - папку **Задачи**;
   - папку группы администрирования;
   - папку **Учетные записи пользователей**;
   - папку **Удаленные объекты**;
   - подпапку **Инсталляционные пакеты**, вложенную в папку **Удаленная установка**.

2. В зависимости от местоположения соответствующего объекта выполните одно из следующих действий:

   - Если объект находится в узле **Сервер администрирования** или в папке группы администрирования, выберите пункт **Свойства** в контекстном меню объекта.

   - Если объект находится в папке **Политики**, **Задачи**, **Учетные записи пользователей**, **Удаленные объекты** или **Инсталляционные пакеты**, выберите папку и в соответствующей рабочей области выберите объект.

   Откроется окно свойств объекта.

3. В панели **Разделы** выберите раздел **История ревизий**.

   История ревизий отображается в рабочей области.

Сравнение ревизий объекта

Вы можете сравнить предыдущие ревизии объекта с текущей ревизией, сравнить ревизии, выбранные в списке, или сравнить ревизию объекта с ревизией другого однотипного объекта.

Чтобы сравнить ревизии объекта:

1. Выберите объект и перейдите к окну свойств этого объекта.

2. В окне свойств задачи выберите раздел **История ревизий**.

3. В рабочей области в списке ревизий объекта выберите ревизию для сравнения.

   Для выбора более двух ревизий объекта используйте клавиши **SHIFT** и **CTRL**.

4. Выполните одно из следующих действий:

   - Нажмите на кнопку **Сравнить** и в раскрывающемся списке выберите одно из значений:

     - **Сравнить с текущей ревизией**

       Выберите этот вариант, чтобы сравнить выбранную ревизию с текущей.

     - **Сравнить выбранные ревизии**

       Выберите этот вариант, чтобы сравнить две выбранные ревизии.

     - **Сравнить с другой задачей**

       При работе с ревизиями задач выберите вариант **Сравнить с другой задачей**, чтобы сравнить выбранную ревизию с ревизией другой задачи.

       При работе с ревизиями политик выберите вариант **Сравнить с другой политикой**, чтобы сравнить выбранную ревизию с ревизией другой политики.

   - Откройте окно свойств требуемой ревизии двойным щелчком мыши. В открывшемся окне свойств ревизии нажмите на одну из следующих кнопок:

     - **Сравнить с текущей**

       Нажмите на эту кнопку, чтобы сравнить выбранную ревизию с текущей.

- **Сравнить с предыдущей**

  Нажмите на эту кнопку, чтобы сравнить выбранную ревизию с предыдущей.

Отчет о сравнении ревизий в формате HTML отображается в вашем браузере по умолчанию.

В отчете можно свернуть некоторые блоки параметров ревизии. Чтобы свернуть блок параметров ревизии, нажмите на значок стрелки (▲) рядом с названием блока.

В ревизии Сервера администрирования попадает информация об изменениях, кроме информации из следующих областей:

- раздела **Трафик**;
- раздела **Правила назначения тегов**;
- раздела **Уведомление**;
- раздела **Точки распространения**;
- раздела **Вирусная атака**.

  Из раздела **Вирусная атака** не будет записана информация о настройке активации политик по событию Вирусная атака.

Вы можете сравнивать ревизии удаленного объекта с ревизией существующего объекта, но не наоборот: вы не можете сравнивать ревизии существующего объекта с ревизией удаленного объекта.

Установка срока хранения ревизий объектов и информации об удаленных объектах

Срок хранения ревизий объекта такой же, как срок хранения информации об удаленных объектах. Срок, заданный по умолчанию, – 90 дней. Этого достаточно для регулярного аудита приложения.

Только пользователи с правами **Изменение** в области **Удаленные объекты** могут изменить срок хранения ревизий объектов и информации об удаленных объектов.

Чтобы изменить срок хранения ревизий объектов и информации об удаленных объектах:

1. В дереве консоли выберите Сервер администрирования, для которого нужно изменить срок хранения ревизий объектов и информации об удаленных объектах.
2. В контекстном меню объекта выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Хранилище истории ревизий** укажите требуемый срок хранения (в днях).
4. Нажмите на кнопку **ОК**.

Ревизии объектов и информация об удаленных объектах будут храниться указанное количество дней.

Просмотр ревизии объекта

Если вам понадобилось узнать, какие изменения проводились с объектом в определенный период, вы можете просмотреть ревизии объекта.

Чтобы просмотреть ревизии объекта:

1. Перейдите к разделу **История ревизий** объекта.
2. В списке ревизий объекта выберите ревизию, параметры которой нужно посмотреть.
3. Выполните одно из следующих действий:
   - Нажмите на кнопку **Просмотреть ревизию**.
   - Откройте окно свойств ревизии двойным щелчком мыши по названию ревизии и нажмите на кнопку **Просмотреть ревизию**.

Отобразится отчет с параметрами выбранной ревизии объекта в формате HTML. В отчете можно свернуть некоторые блоки параметров ревизии объекта. Чтобы свернуть блок параметров ревизии, нажмите на значок стрелки (▲) рядом с названием блока.

Сохранение ревизии объекта в файле

Вы можете сохранить ревизию объекта в текстовом файле, например, чтобы отправить файл по электронной почте.

Чтобы сохранить ревизию объекта в файле:

1. Перейдите к разделу **История ревизий** объекта.
2. В списке ревизий объекта выберите ревизию, параметры которой нужно сохранить.
3. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Сохранить в файл**.

Ревизия будет сохранена в файле формата TXT.

Откат изменений

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. Перейдите к разделу **История ревизий** объекта.
2. В списке ревизий объекта выберите номер ревизии, к которой нужно откатить изменения.
3. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Откатить**.

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.

Добавление описания ревизии

Вы можете добавить описание для ревизии, чтобы в дальнейшем было проще найти необходимую ревизию в списке.

Чтобы добавить описание ревизии:

1. Перейдите к разделу **История ревизий** объекта.
2. В списке ревизий объекта выберите ревизию, для которой нужно добавить описание.
3. Нажмите на кнопку **Описание**.
4. В окне **Описание ревизии объекта** введите текст описания ревизии.

   По умолчанию описание ревизии объекта не заполнено.
5. Нажмите на кнопку **ОК**.

Удаление объектов

В этом разделе приведена информация об удалении объектов.

Вы можете удалять следующие объекты:

- политики;
- задачи;
- инсталляционные пакеты;
- виртуальные Серверы администрирования;
- пользователей;
- группы безопасности;
- группы администрирования.

Чтобы удалить объект:

1. Откройте нужный раздел в Kaspersky Security Center Web Console и выберите объект.
2. В панели инструментов нажмите на кнопку **Удалить**.
3. В появившемся окне нажмите на кнопку **OK**, чтобы подтвердить свой выбор.

   Выбранный объект будет удален.

Когда вы удаляете объект, информация об этом записывается в базу данных. Срок хранения информации об удаленных объектах такой же, как и срок хранения ревизий объектов (рекомендуемый срок 90 дней). Можно изменить время хранения только при наличии права на **Изменение** для области **Удаленные объекты**.

Об удалении клиентских устройств

При удалении управляемого устройства из группы администрирования приложение перемещает устройство в группу Нераспределенные устройства. После удаления устройства установленные приложения "Лаборатории Касперского" – Агент администрирования и приложение безопасности, например Kaspersky Endpoint Security, – остаются на устройстве.

Kaspersky Security Center обрабатывает устройства из группы Нераспределенные устройства по следующим правилам:

- Если вы настроили правила перемещения устройств и устройство соответствует критериям правила перемещения, устройство автоматически перемещается в группу администрирования в соответствии с правилом.
- Устройство сохраняется в группе Нераспределенные устройства и автоматически удаляется из группы в соответствии с правилами хранения устройств.

  Правила хранения устройств не влияют на устройства, на которых один или несколько дисков зашифрованы с помощью полнодискового шифрования. Такие устройства не удаляются автоматически – вы можете удалить их только вручную. Если вам нужно удалить устройство с зашифрованным жестким диском, сначала расшифруйте диск, а затем удалите устройство.

  > При удалении устройства с зашифрованным жестким диском данные, необходимые для расшифровки диска, также удаляются. Если вы установите флажок **Я понимаю риск и хочу удалить выбранные устройства** в окне подтверждения, которое открывается при удалении таких устройств (из группы **Нераспределенные устройства** или из группы **Управляемые устройства**), это означает, что вы знаете о последующем удалении данных.

  В этом случае для расшифровки диска требуется выполнение следующих условий:

  - Устройство повторно подключается к Серверу администрирования для восстановления данных, необходимых для расшифровки диска.
  - Пользователь устройства помнит пароль для расшифровки.
  - Приложение безопасности, которое использовалось для шифрования диска, например Kaspersky Endpoint Security для Windows, установлено на устройстве.

Если диск был зашифрован с помощью технологии Kaspersky Disk Encryption, вы также можете попробовать восстановить данные с помощью утилиты FDERT Restore.

В VDI, если у вас есть устройство с зашифрованными жесткими дисками, информация на зашифрованном диске удаляется после удаления устройства.

При удалении устройства из группы Нераспределенные устройства вручную приложение удаляет устройство из списка. После удаления устройства установленные приложения "Лаборатории Касперского" (если они есть) остаются на устройстве. Затем, если устройство по-прежнему видно Серверу администрирования и вы настроили регулярный опрос сети, Kaspersky Security Center 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.

Удаление объекта

Вы можете удалять объекты, такие как политики, задачи, инсталляционные пакеты, внутренних пользователей и внутренние группы безопасности, если у вас есть права на изменение для категории Базовая функциональность (подробную информацию см. в статье Назначение прав пользователям и группам пользователей).

Вы не можете удалить инсталляционные пакеты, которые используются в задачах удаленной установки. Сначала необходимо остановить соответствующие задачи. Подробнее о задаче автоматической установки в группах администрирования см. в статье Автоматическая установка приложений на устройства группы администрирования.

Чтобы удалить объект:

1. В рабочей области требуемой папки дерева консоли выберите объект.
2. Выполните одно из следующих действий:
   - В контекстном меню объекта выберите пункт **Удалить**.
   - Нажмите на кнопку **DELETE**.

Объект будет удален, и информация об этом будет записана в базу данных.

Просмотр информации об удаленных объектах

Информация об удаленных объектах хранится в папке Удаленные объекты такой же срок, как и ревизии объекта (рекомендуемый срок составляет 90 дней).

Только пользователи с правами на **Чтение** для области **Удаленные объекты** могут просматривать список удаленных объектов (подобную информацию см. в разделе Назначение прав пользователям и группам пользователей).

Чтобы просмотреть список удаленных объектов,

В дереве консоли выберите пункт **Удаленные объекты** (по умолчанию папка **Удаленные объекты** вложена в папку **Дополнительно**).

Если у вас нет прав на чтение для области **Удаленные объекты**, в папке **Удаленные объекты** будет отображаться пустой список.

В рабочей области папки **Удаленные объекты** содержится следующая информация об удаленных объектах:

- **Название**. Название удаленного объекта.
- **Тип**. Тип объекта, такой как политика, задача или инсталляционный пакет.
- **Время**. Время, когда объект был удален.
- **Пользователь**. Учетная запись пользователя, который удалил объект.

Чтобы просмотреть больше информации об удаленном объекте:

1. В дереве консоли выберите пункт **Удаленные объекты** (по умолчанию папка **Удаленные объекты** вложена в папку **Дополнительно**).
2. В рабочей области папки **Удаленные объекты** выберите нужный объект.

   В правой части рабочей области отобразится поле для работы с выбранным объектом.
3. Выполните одно из следующих действий:

   - Перейдите по ссылке **Свойства** в блоке работы с выбранным объектом.
   - В контекстном меню объекта выберите пункт **Свойства**.

   Откроется окно свойств объекта, в котором отображается следующая информация:

   - **Общие**
   - **История ревизий**

Удаление объектов из списка удаленных объектов

Только пользователи с правами **Изменение** для области **Удаленные объекты** могут удалять объекты из списка удаленных объектов (подобную информацию см. в разделе Назначение прав пользователям и группам пользователей).

Чтобы удалить объект из списка удаленных объектов:

1. В дереве консоли выберите узел нужного Сервера администрирования и выберите папку **Удаленные объекты**.
2. В рабочей области папки выберите объект или объекты, которые вы хотите удалить.

3. Выполните одно из следующих действий:

   - Нажмите на кнопку **DELETE**.
   - В контекстном меню объекта или объектов, которые вы выбрали, выберите пункт **Удалить**.

4. В диалоговом окне нажмите на кнопку **Да**.

   Объект удален из списка удаленных объектов. Вся информация объекта (включая все ревизии) удалена из базы данных. Вы не можете восстановить эту информацию.

Управление мобильными устройствами

Управление защитой мобильными устройствами через Kaspersky Security Center выполняется с помощью компонента Управление мобильными устройствами. Если вы планируете управлять мобильными устройствами, принадлежащими сотрудникам вашей организации, вам нужно включить Управление мобильными устройствами.

В этом разделе приведены инструкции по включению, настройке и отключению Управления мобильными устройствами. В этом разделе также описано управление мобильными устройствами, подключенными к Серверу администрирования.

Подробнее о Kaspersky Security для мобильных устройств см. в *справке Kaspersky Security для мобильных устройств*.

Сценарий: развертывание Управления мобильными устройствами

В этом разделе приведен сценарий для настройки возможностей Управления мобильными устройствами в Kaspersky Security Center.

Предварительные требования

Убедитесь, что ваша лицензия предоставляет доступ к возможностям Управления мобильными устройствами.

Этапы

Развертывание возможностей Управления мобильными устройствами состоит из следующих этапов:

1. **Подготовка портов**

   Убедитесь, что на Сервере администрирования доступен порт 13292. Этот порт требуется для подключения мобильных устройств. Также вы можете сделать доступным порт 17100. Этот порт требуется только для активации прокси-сервера для управляемых мобильных устройств; если управляемые мобильные устройства имеют доступ в интернет, этот порт доступным делать не требуется.

2. **Включение Управления мобильными устройствами**

   Вы можете включить Управление мобильными устройствами во время запуска мастера первоначальной настройки Сервера администрирования или позже.

3. **Указание внешнего адреса Сервера администрирования**

   Вы можете указать внешний адрес во время запуска мастера первоначальной настройки Сервера администрирования или позже. Если вы не выбрали Управление мобильными устройствами для установки и не указали адрес в мастере установки приложения, укажите внешний адрес в свойствах инсталляционного пакета.

4. **Добавление мобильных устройств в группу Управляемые устройства**

   Добавьте мобильные устройства в группу Управляемые устройства, чтобы управлять этими устройствами с помощью политик. Вы можете создать правило перемещения на одном из шагов мастера первоначальной настройки Сервера администрирования. Также вы можете создать правило перемещения позже. Если вы не создадите такое правило, вы можете добавить мобильные устройства в группу Управляемые устройства вручную.

   Вы можете добавить мобильные устройства в группу Управляемые устройства напрямую или создать для них подгруппу (или несколько подгрупп).

   Позже, в любое время вы можете подключить новое мобильное устройство к Серверу администрирования с помощью мастера подключения мобильного устройства.

5. **Создание политики для мобильных устройств**

   Чтобы управлять мобильными устройствами, создайте политику (или несколько политик) для этих устройств в группе, к которой они принадлежат. Вы можете изменить параметры политики в любое время.

Результаты

После завершения сценария вы сможете управлять устройствами Android и iOS, используя Kaspersky Security Center. Вы можете работать с сертификатами мобильных устройств и отправлять команды на мобильные устройства.

О групповых политиках для управления iOS MDM-устройствами

Для управления iOS MDM-устройствами вы можете использовать плагин управления Kaspersky Device Management для iOS, входящий в комплект поставки Kaspersky Security Center. Kaspersky Device Management для iOS позволяет создавать групповые политики для настройки конфигурационных параметров iOS MDM-устройств без использования iPhone Configuration Utility.

Групповая политика для управления iOS MDM-устройствами позволяет администратору:

- настраивать параметры безопасности использования пароля на устройстве;
- настраивать ограничения для использования аппаратных функций устройства, а также ограничения на установку, удаление мобильных приложений;
- настраивать ограничения для использования на устройстве встроенных мобильных приложений, например, YouTube™, iTunes Store или Safari;
- настраивать ограничения просмотра медиаконтента (например, фильмов и TV-шоу) по региону местоположения устройства;

- настраивать параметры подключения устройства к интернету через прокси-сервер (Глобальный HTTP-прокси);
- настраивать параметры единой учетной записи, с помощью которой пользователь может получить доступ к корпоративным приложениям и сервисам (технология единого входа);
- контролировать использование интернета (посещение веб-сайтов) на мобильных устройствах;
- настраивать параметры беспроводных сетей (Wi-Fi), точек доступа (APNs), виртуальных частных сетей (VPN) с использованием различных механизмов аутентификации и сетевых протоколов;
- настраивать параметры подключения к устройствам AirPlay для потоковой передачи фотографий, музыки и видео;
- настраивать параметры подключения к принтерам AirPrint™ для печати документов с устройства беспроводным способом;
- настраивать параметры синхронизации с сервером Microsoft Exchange, а также учетные записи пользователей для использования корпоративной почты на устройствах;
- настраивать учетные данные пользователя для синхронизации со службой каталогов LDAP;
- настраивать учетные данные пользователя для подключения к сервисам CalDAV и CardDAV, что позволяет пользователю использовать корпоративные календари и списки контактов;
- настраивать параметры интерфейса iOS на устройстве пользователя, например, шрифты или иконки для избранных веб-сайтов;
- добавлять новые сертификаты безопасности на устройство;
- настраивать параметры SCEP-сервера (Simple Certificate Enrollment Protocol) для автоматического получения устройством сертификатов из Центра сертификации;
- добавление собственных параметров для работы мобильных приложений.

Особенностью политики управления iOS MDM-устройствами является то, что она назначается группе администрирования, в которую входит Сервер iOS MDM (далее "Сервер мобильных устройств"). Все параметры, заданные в этой политике, сначала распространяются на Сервер мобильных устройств, затем на мобильные устройства, которыми управляет этот сервер. В случае использования иерархической структуры групп администрирования подчиненные серверы мобильных устройств получают параметры политики от главных серверов мобильных устройств и распространяют их на мобильные устройства.

Дополнительную информацию об использовании групповой политики для управления iOS MDM-устройствами с помощью Консоли администрирования Kaspersky Security Center см. в *справке Kaspersky Security для мобильных устройств*.

Включение Управления мобильными устройствами

Для управления мобильными устройствами необходимо включить Управление мобильными устройствами. Если вы не включили Управление мобильными устройствами в мастере первоначальной настройки, вы можете сделать это позже. Управление мобильными устройствами требует лицензии.

Включение Управления мобильными устройствами доступно только на главном Сервере администрирования.

Чтобы включить Управление мобильными устройствами:

1. В дереве консоли выберите папку **Управление мобильными устройствами**.

2. По кнопке **Включить Управление мобильными устройствами** в рабочей области папки запустите мастер создания задачи. Эта кнопка доступна, только если вы ранее не включали **Управление мобильными устройствами**.

   Отобразится окно **Дополнительные компоненты** мастера первоначальной настройки Сервера администрирования.

3. Для управления мобильными устройствами выберите **Включить Управление мобильными устройствами**.

4. В окне **Выбор способа активации приложения** произведите активацию приложения с помощью файла ключа или кода активации.

   Управление мобильными устройствами будет недоступно, пока вы не активируете возможность Управления мобильными устройствами.

5. На странице **Параметры прокси-сервера для получения доступа в интернет** установите флажок **Использовать прокси-сервер**, если вы хотите использовать прокси-сервер для подключения к интернету. Если флажок установлен, становятся доступны поля ввода параметров. Настройте параметры подключения к прокси-серверу.

6. На странице **Проверка обновлений для плагинов и инсталляционных пакетов** выберите один из следующих вариантов:

   - **Проверить актуальность плагинов и инсталляционных пакетов**

     Запуск проверки на актуальность. Если проверка обнаружит использование устаревших версий плагинов или инсталляционных пакетов, мастер предложит загрузить актуальные версии вместо устаревших.

   - **Пропустить проверку**

     Продолжение работы без проверки плагинов и инсталляционных пакетов на актуальность. Этот вариант можно выбрать, например, если у вас нет доступа в интернет или вы по какой-то причине хотите продолжить пользоваться устаревшей версией программы.

     > Пропуск проверки актуальности плагинов может привести к некорректной работе приложения.

7. В окне **Доступные последние версии плагинов** загрузите и установите последние версии плагинов на необходимом вам языке. Для обновления плагина не требуется лицензии.

   После установки плагинов и пакетов приложение проверяет, все ли необходимые плагины для корректной работы мобильных устройств были установлены. Если обнаружатся устаревшие версии плагинов, то мастер предложит загрузить актуальные версии вместо устаревших.

8. На странице **Параметры подключения мобильных устройств** настройте порты Сервера администрирования Сервера администрирования.

После завершения работы мастера будут выполнены следующие изменения:

- создана политика Kaspersky Endpoint Security для Android;
- создана политика Kaspersky Device Management для iOS;
- открыты порты Сервера администрирования для мобильных устройств.

Изменение параметров Управления мобильными устройствами

Чтобы включить поддержку мобильных устройств:

1. В дереве консоли выберите папку **Управление мобильными устройствами**.
2. В рабочей области папки перейдите по ссылке **Порты подключения для мобильных устройств**.

   Отобразится раздел **Дополнительные порты** окна свойств Сервера администрирования.

3. В разделе **Дополнительные порты** измените необходимые вам параметры:

   - SSL-порт для прокси-сервера активации
   - **Открыть порт для мобильных устройств**

     Если флажок установлен, то открыт порт, по которому мобильные устройства будут подключаться к Серверу лицензирования. Вы можете задать номер порта и другие настройки в полях ниже.

     Если флажок снят, то открытого порта для подключения мобильных устройств нет, и поля **Порт для мобильных устройств** и **Порт активации мобильных клиентов** недоступны для редактирования.

     По умолчанию флажок установлен.

   - **Порт для синхронизации мобильных устройств**

     Номер порта, по которому мобильные устройства будут подключаться к Серверу администрирования и обмениваться с ним информацией. По умолчанию используется порт 13292.

     Вы можете назначить другой порт, если порт 13292 используется в каких-то других целях.

   - **Порт для активации мобильных устройств**

     Порт подключения Kaspersky Endpoint Security для Android к серверам активации "Лаборатории Касперского".

     По умолчанию используется порт 17100.

4. Нажмите на кнопку **OK**.

Выключение Управления мобильными устройствами

Выключение Управления мобильными устройствами доступно только на главном Сервере администрирования.

Чтобы выключить Управления мобильными устройствами:

1. В дереве консоли выберите папку **Управление мобильными устройствами**.
2. В рабочей области папки перейдите по ссылке **Настроить дополнительные компоненты**.

   Отобразится окно **Дополнительные компоненты** мастера первоначальной настройки Сервера администрирования.
3. Выберите пункт **Не включать Управление мобильными устройствами**, если вы больше не хотите управлять мобильными устройствами.
4. Нажмите на кнопку **OK**.

Ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования. Порт подключения мобильных устройств и порт активации мобильных устройств будут закрыты автоматически.

Созданные политики Kaspersky Endpoint Security для Android и Kaspersky Device Management для iOS не будут удалены. Правила выпуска сертификатов не изменяются. Установленные плагины не удаляются. Правило перемещения мобильных устройств не будет удалено.

После повторного включения Управления мобильными устройствами на управляемых мобильных устройствах может потребоваться переустановка мобильных приложений, которые необходимы для управления мобильными устройствами.

Работа с командами для мобильных устройств

Этот раздел содержит информацию о командах для управления мобильными устройствами, которые поддерживает Kaspersky Security Center. В разделе приведены инструкции по отправке команд на мобильные устройства, а также по просмотру статуса выполнения команд в журнале команд.

Команды для управления мобильными устройствами

Kaspersky Security Center поддерживает команды для управления мобильными устройствами.

Команды используются для дистанционного управления мобильными устройствами. Например, в случае потери мобильного устройства с помощью команды можно удалить корпоративные данные с устройства.

Вы можете использовать команды для следующих типов управляемых мобильных устройств:

- iOS MDM-устройства;
- KES-устройства.

Каждый тип устройства поддерживает свой набор команд.

Особенности некоторых команд

- Для всех типов устройств в случае успешного выполнения команды **Сбросить настройки до заводских** все данные будут удалены с устройства, настройки устройства будут сброшены до заводских.
- Для iOS MDM-устройств в случае успешного выполнения команды **Удалить корпоративные данные** с устройства будут удалены все установленные конфигурационные профили, provisioning-профили, iOS MDM-профиль и приложения, для которых был установлен флажок **Удалять вместе с iOS MDM-профилем**.
- Для KES-устройств в случае успешного выполнения команды **Удалить корпоративные данные** с устройства будут удалены корпоративные данные, записи в Контактах, история SMS, журнал вызовов, календарь, параметры подключения к интернету, учетные записи пользователя, кроме учетной записи Google™. Для KES-устройств дополнительно будут удалены данные с карты памяти.
- Перед отправкой команды **Определить местоположение** на KES-устройство вам потребуется подтвердить, что вы используете эту команду для санкционированного поиска потерянного устройства, принадлежащего вашей организации или одному из сотрудников. Мобильное устройство, принимающее команду **Определить местоположение** не заблокировано.

Список команд для мобильных устройств

В таблице ниже приведен список команд для iOS MDM-устройств.

Список поддерживаемых команд для управления мобильными устройствами: iOS MDM-устройства

Команды	Результат выполнения команды
Заблокировать	Мобильное устройство заблокировано.
Разблокировать	Выключена блокировка мобильного устройства PIN-кодом. Установленный ранее PIN-код сброшен.
Сбросить настройки до заводских	Удалены все данные с мобильного устройства, настройки мобильного устройства сброшены до заводских.
Удалить корпоративные данные	Удалены все установленные конфигурационные профили, provisioning-профили, iOS MDM-профиль и приложения, для которых был установлен флажок **Удалять вместе с iOS MDM-профилем**.
Синхронизировать устройство	Данные мобильного устройства синхронизированы с Сервером администрирования.
Установить профиль	Конфигурационный профиль установлен на мобильное устройство.
Удалить профиль	Конфигурационный профиль удален с мобильного устройства.
Установить provisioning-профиль	Provisioning-профиль установлен на мобильное устройство.
Удалить provisioning-профиль	Provisioning-профиль удален с мобильного устройства.
Установить приложение	Приложение установлено на мобильное устройство.
Удалить приложение	Приложение удалено с мобильного устройства.

Команды	Результат выполнения команды
Ввести код погашения	Введен код погашения для платного приложения.
Настроить параметры роуминга	Включен или выключен роуминг данных и голосовой роуминг.

В таблице ниже приведен список команд для KES-устройств.

Список поддерживаемых команд для управления мобильными устройствами: iOS MDM-устройства

Команда	Результат выполнения команды
Заблокировать	Мобильное устройство заблокировано.
Разблокировать	Выключена блокировка мобильного устройства PIN-кодом. Установленный ранее PIN-код сброшен.
Сбросить настройки до заводских	Удалены все данные с мобильного устройства, настройки мобильного устройства сброшены до заводских.
Удалить корпоративные данные	Удалены корпоративные данные, записи в Контактах, история SMS, журнал вызовов, календарь, параметры подключения к интернету, учетные записи пользователя, кроме учетной записи Google. Удалены данные с карты памяти.
Синхронизировать устройство	Данные мобильного устройства синхронизированы с Сервером администрирования.
Определить местоположение устройства	Местоположение мобильного устройства определено и показано на Google Картах™. Оператор мобильной связи взимает оплату за передачу SMS и интернет.
Сфотографировать	Мобильное устройство заблокировано. Фотография выполнена фронтальной камерой устройства и сохранена на Сервере администрирования. Фотографии доступны для просмотра в журнале команд. Оператор мобильной связи взимает оплату за передачу SMS и интернет.
Воспроизвести звуковой сигнал	Мобильное устройство воспроизводит звуковой сигнал.

Использование Firebase Cloud Messaging

Для своевременной доставки команд на KES-устройства под управлением операционной системы Android в Kaspersky Security Center используется механизм push-нотификаций. Push-нотификации между KES-устройствами и Сервером администрирования осуществляются с помощью сервиса Firebase Cloud Messaging (далее – FCM). В Консоли администрирования Kaspersky Security Center вы можете указать параметры сервиса Cloud Messaging, чтобы подключить KES-устройства к этому сервису.

Для получения параметров Firebase Cloud Messaging вам необходимо иметь учетную запись Google.

Чтобы включить использование FCM:

1. В Консоли администрирования выберите узел **Управление мобильными устройствами** и папку **Мобильные устройства**.
2. В контекстном меню папки **Мобильные устройства** выберите пункт **Свойства**.
3. В окне свойств папки выберите раздел **Параметры Firebase Cloud Messaging**.
4. В поле **Номер проекта Firebase** укажите Sender ID FCM.
5. В поле **Файл приватного ключа (в формате JSON)** выберите файл приватного ключа.

При следующей синхронизации с Сервером администрирования KES-устройства под управлением операционной системы Android будут подключены к службе Firebase Cloud Messaging.

Вы можете изменить параметры Firebase Cloud Messaging по кнопке **Сбросить параметры**.

Отправка команд

Чтобы отправить команду на мобильное устройство пользователя:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. Выберите мобильное устройство пользователя, на которое нужно отправить команду.

3. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

4. В окне **Команды для управления мобильным устройством** перейдите в раздел с названием команды, которую нужно отправить на мобильное устройство, и нажмите на кнопку **Отправить команду**.

   В зависимости от выбранной команды после нажатия на кнопку **Отправить команду** может открыться окно настройки дополнительных параметров команды. Например, при отправке команды на удаление с мобильного устройства provisioning-профиля приложение предлагает выбрать provisioning-профиль, который нужно удалить с мобильного устройства. Укажите в окне дополнительные параметры команды и подтвердите свой выбор. После этого команда будет отправлена на мобильное устройство.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

   По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

   В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

5. Нажмите на кнопку **ОК**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Просмотр статусов команд в журнале команд

Приложение сохраняет информацию о всех командах, отправленных на мобильные устройства, в журнале команд. В журнале команд сохраняется информация о времени и дате отправления команд на мобильное устройство, статусы команд, а также подробные описания результатов выполнения команд. Например, в случае неудачного выполнения команды в журнале отображается причина ошибки. Записи в журнале команд хранятся не более 30 дней.

Команды, отправленные на мобильные устройства, могут иметь следующие статусы:

- *Выполняется* – команда отправлена на мобильное устройство.
- *Завершена* – выполнение команды успешно завершено.
- *Завершена с ошибкой* – выполнить команду не удалось.
- *Удаляется* – команда удаляется из очереди команд, отправленных на мобильное устройство.

- *Удалена* – команда успешно удалена из очереди команд, отправленных на мобильное устройство.
- *Удаление завершено с ошибкой* – команду не удалось удалить из очереди команд, отправленных на мобильное устройство.

Приложение ведет журнал команд для каждого мобильного устройства.

Чтобы просмотреть журнал команд, отправленных на мобильное устройство:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. Выберите в списке мобильное устройство, для которого вы хотите просмотреть журнал команд.

3. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

   Откроется окно **Команды для управления мобильным устройством**. Разделы окна **Команды для управления мобильным устройством** соответствуют командам, которые можно отправить на мобильное устройство.

4. Выбирайте разделы с нужными вам командами и просматривайте информацию об отправке и выполнении команд в блоке **Журнал команд**.

В блоке **Журнал команд** можно просмотреть список команд, отправленных на мобильное устройство, и информацию о командах. С помощью фильтра **Показать команды** можно показывать в списке только команды с выбранным статусом.

Работа с сертификатами для мобильных устройств

Этот раздел содержит информацию о работе с сертификатами мобильных устройств.

Срок действия корневого сертификата для мобильных устройств составляет 700 дней после его создания. Резервный сертификат создается за 60 дней до истечения срока действия. Вы можете изменить время создания резервного сертификата с помощью следующей команды:

```
klscflag.exe -fset -pv klserver -n KLSRV_AKLWNGT_MDM_CERT_CHANGE_TIMEOUT -t d -v <время ожидания в секундах>
```

Время создания резервного сертификата должно быть достаточным, чтобы все управляемые мобильные устройства синхронизировались с Сервером администрирования и получили сертификат.

Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Обновление корневого сертификата для мобильных устройств вручную не поддерживается.

Запуск мастера установки сертификата

Вы можете устанавливать на мобильное устройство пользователя сертификаты следующих типов:

- общие сертификаты для идентификации мобильного устройства;
- почтовые сертификаты для настройки на мобильном устройстве корпоративной почты;
- VPN-сертификат для настройки на мобильном устройстве доступа к виртуальной частной сети.

Чтобы установить сертификат на мобильное устройство пользователя:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Сертификаты**.
2. В рабочей области папки **Сертификаты** по ссылке **Добавить сертификат** запустите мастер установки сертификата.

   Следуйте далее указаниям мастера.

В результате работы мастера сертификат будет создан, добавлен в список пользовательских сертификатов, кроме того, будет отправлено уведомление пользователю со ссылкой для загрузки и установки сертификата на мобильное устройство. Список всех сертификатов можно просмотреть и экспортировать в файл. Можно удалять и перевыпускать сертификаты, а также просматривать их свойства.

Шаг 1. Выбор типа сертификата

Укажите тип сертификата, который необходимо установить на мобильное устройство пользователя:

- **Мобильный сертификат** – для идентификации мобильного устройства.
- **Почтовый сертификат** – для настройки на мобильном устройстве корпоративной почты.
- **VPN-сертификат** – для настройки на мобильном устройстве доступа к виртуальной частной сети.

Шаг 2. Выбор типа устройства

Это окно отображается, только если ранее был выбран тип сертификата **Почтовый сертификат** или **VPN-сертификат**.

Укажите тип операционной системы устройства:

- **iOS MDM-устройство**. Выберите этот вариант, если необходимо установить сертификат на мобильное устройство, которое подключается к Серверу iOS MDM по протоколу iOS MDM.

- **KES-устройство под управлением Kaspersky Security для мобильных устройств**. Выберите этот вариант, если необходимо установить сертификат на KES-устройство. В этом случае сертификат будет использоваться при подключении к Серверу администрирования для идентификации пользователя.

- **KES-устройство, которое подключается к Серверу администрирования без аутентификации по пользовательскому сертификату**. Выберите этот вариант, если необходимо установить сертификат на KES-устройство без аутентификации по сертификату. В этом случае на последнем шаге мастера в окне **Способ уведомления пользователей** администратор должен выбрать тип авторизации пользователя при подключении к Серверу администрирования.

Шаг 3. Выбор пользователя

Выберите в списке пользователей, группы безопасности или группы безопасности Active Directory, для которых вы хотите установить сертификат.

В окне **Выбор пользователя** можно выполнить поиск внутренних пользователей Kaspersky Security Center. Вы можете нажать на кнопку **Добавить**, чтобы добавить внутреннего пользователя.

Шаг 4. Выбор источника сертификата

В окне можно выбрать источник сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Можно задать сертификат одним из следующих способов:

- Автоматически создать сертификат средствами Сервера администрирования и доставить сертификат на устройство.

- Указать файл ранее созданного сертификата. Этот способ недоступен, если на предыдущем шаге было выбрано несколько пользователей.

Установите флажок **Опубликовать сертификат**, если необходимо отправить уведомление пользователю о создании сертификата для его мобильного устройства.

Если мобильное устройство пользователя уже было авторизовано по сертификату ранее и нет необходимости указывать имя учетной записи и пароль для получения нового сертификата, снимите флажок **Опубликовать сертификат**. В этом случае окно **Способ уведомления пользователей** отображаться не будет.

Шаг 5. Назначение тега сертификатам

Окно **Тег сертификата** отображается, если в поле **Тип устройства** выбрано значение **iOS MDM-устройство**.

В раскрывающемся списке вы можете назначить тег для сертификата iOS MDM-устройства пользователя. Сертификат с назначенным тегом может иметь специальные параметры, установленные для этого тега в свойствах политики Kaspersky Device Management для iOS.

Для выбора в раскрывающемся списке доступны теги *Шаблон сертификата 1*, *Шаблон сертификата 2* и *Шаблон сертификата 3*, параметры которых могут быть настроены в следующих разделах:

- Если в окне **Тип сертификата** был выбран тип **Почтовый сертификат**, параметры тегов для него настраиваются в свойствах учетной записи Exchange ActiveSync для мобильных устройств (**Управляемые устройства** → **Политики** → Свойства политики Kaspersky Device Management для iOS → Раздел **Exchange ActiveSync** → **Добавить** → **Дополнительно**).

- Если в окне **Тип сертификата** был выбран тип **VPN-сертификат**, параметры тегов для него настраиваются в свойствах сети VPN для мобильных устройств (**Управляемые устройства** → **Политики** → Свойства политики Kaspersky Device Management для iOS → Раздел **VPN** → **Добавить** → **Дополнительно**). Настройка тегов, используемых для VPN-сертификатов, недоступна, если для сети VPN выбран тип соединения L2TP, PPTP, или IPSec (Cisco™).

Шаг 6. Описание параметров публикации сертификата

В этом окне вы можете указать следующие параметры публикации сертификата:

- **Не уведомлять пользователя о новом сертификате**

  Включите этот параметр, если вы не хотите отправлять пользователю уведомление о создании сертификата для его мобильного устройства. В этом случае окно **Способ уведомления пользователя** отображаться не будет.

  > Этот параметр применим только к устройствам с установленным приложением Kaspersky Endpoint Security для Android.

  Возможно, вы захотите включить этот параметр, например, если мобильное устройство пользователя уже было идентифицировано с помощью сертификата, поэтому нет необходимости указывать имя учетной записи и пароль для получения нового сертификата.

- **Разрешить устройству получать один и тот же сертификат несколько раз (только для устройств с установленным Kaspersky Endpoint Security для Android)**

  Включите этот параметр, чтобы Kaspersky Security Center автоматически повторно отправлял сертификат каждый раз, когда срок его действия истекает в ближайшее время или не найден на целевом устройстве.

  Сертификат автоматически отправляется повторно за несколько дней до истечения срока действия сертификата. Вы можете установить количество дней в окне Правила выпуска сертификатов.

  В некоторых случаях сертификаты не могут быть найдены на устройствах. Например, это может произойти, если пользователь заново установит приложение безопасности "Лаборатории Касперского" на устройство или сбросит настройки устройства до заводских. В этом случае Kaspersky Security Center проверяет идентификатор устройства при следующей попытке устройства подключиться к Серверу администрирования. Если устройство имеет такой же идентификатор, как и при выдаче сертификата, приложение передает сертификат на устройство.

Шаг 7. Выбор способа уведомления пользователей

Это окно не отображается, если в качестве типа устройства выбран вариант **iOS MDM-устройство** или если выбран вариант **Не уведомлять пользователя о новом сертификате**.

В окне **Способ уведомления пользователей** можно настроить параметры уведомления пользователя об установке сертификата на мобильное устройство.

В поле **Тип авторизации** укажите тип аутентификации пользователя:

- **Учетные данные (доменные или псевдонима)**

  В этом случае пользователь использует доменный пароль или пароль внутреннего пользователя Kaspersky Security Center, для того чтобы получить новый сертификат.

- **Одноразовый пароль**

  В этом случае пользователь получит одноразовый пароль, который будет выслан на электронную почту или с помощью SMS. Этот пароль необходимо будет указать для получения нового сертификата.

  Этот параметр изменится на **Пароль**, если вы включили параметр **Разрешить устройству получать один и тот же сертификат несколько раз (только для устройств с установленными приложениями безопасности "Лаборатории Касперского")** в окне **Параметры публикации сертификатов**.

- **Пароль.**

  В этом случае пароль используется каждый раз, когда сертификат отправляется пользователю.

  Этот параметр изменится на **Одноразовый пароль**, если вы включили параметр **Разрешить устройству получать один и тот же сертификат несколько раз (только для устройств с установленными приложениями безопасности "Лаборатории Касперского")** в окне **Параметры публикации сертификатов**.

Это поле отображается, если в окне **Тип сертификата** выбрано значение **Мобильный сертификат** или если в качестве типа устройства выбрано **KES-устройство, которое подключается к Серверу администрирования без аутентификации по пользовательскому сертификату**.

Выберите вариант уведомления пользователя:

- **Показать пароль после завершения работы мастера**

  Если вы выберете этот параметр, имя пользователя, SAM-имя пользователя (Security Account Manager), и пароль для получения сертификата для каждого из выбранных пользователей будут отображаться на последнем шаге мастера установки сертификата. Настройка параметров уведомления пользователя об установленном сертификате будет недоступна.

  Если вы добавляете сертификаты для нескольких пользователей, вы можете сохранить предоставленные учетные данные в файл, нажав на кнопку **Экспорт** на последнем шаге мастера установки сертификата.

  Этот параметр недоступен, если вы выбрали **Учетные данные (доменные или псевдонима)** на шаге **Способ уведомления пользователя** мастера установки сертификата.

- **Сообщить пользователю о новом сертификате**

  При выборе этого варианта вы можете настроить параметры уведомления пользователя о новом сертификате.

  - **По электронной почте**

    В блоке параметров По электронной почте вы можете настроить параметры уведомления пользователя об установке сертификата на его мобильное устройство с помощью сообщений электронной почты. Этот способ оповещения доступен, только если настроен SMTP-сервер.

    Перейдите по ссылке **Изменить сообщение**, чтобы просмотреть и изменить сообщение, если это необходимо.

  - **С помощью SMS**

    В этом блоке параметров вы можете настроить параметры уведомления пользователя об установке сертификата на его мобильное устройство с помощью SMS-сообщений. Этот способ оповещения доступен, только если настроено SMS-оповещение.

    Перейдите по ссылке **Изменить сообщение**, чтобы просмотреть и изменить сообщение, если это необходимо.

Шаг 8. Генерация сертификата

На этом шаге создается сертификат.

Вы можете нажать на кнопку **Готово**, чтобы выйти из мастера.

Сгенерированный сертификат отображается в списке сертификатов в рабочей области папки **Сертификаты**.

Настройка правил выпуска сертификатов

Сертификаты используются для аутентификации устройств на Сервере администрирования. Все управляемые мобильные устройства должны иметь сертификаты. Можно настроить способ выпуска сертификатов.

Чтобы настроить правила выпуска сертификатов:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Сертификаты**.

2. В рабочей области папки **Сертификаты** по кнопке **Настроить правила выпуска сертификатов** откройте окно **Правила выпуска сертификатов**.

3. Перейдите в раздел с названием типа сертификата:

   Выпуск мобильных сертификатов – для настройки выпуска сертификатов для мобильных устройств.

   Выпуск почтовых сертификатов – для настройки выпуска почтовых сертификатов.

   Выпуск VPN-сертификатов – для настройки выпуска VPN-сертификатов.

4. В блоке **Параметры выпуска** настройте выпуск сертификата:

   - Укажите срок действия сертификата в днях.

     Сертификаты для мобильных устройств ограничены сроком действия корневого сертификата. Если вы укажете срок действия сертификата дольше, чем срок действия корневого сертификата, срок действия сертификата будет автоматически изменен при создании.

   - Выберите источник сертификатов (**Сервер администрирования** или **Сертификаты задаются вручную**).

     По умолчанию источником сертификатов выбран Сервер администрирования.

   - Задайте шаблон сертификатов (**Шаблон по умолчанию**, **Другой шаблон**).

     Настройка шаблонов доступна, если в разделе **Интеграция с PKI** настроена интеграция с инфраструктурой открытых ключей.

5. В блоке **Параметры автоматического обновления** настройте автоматическое обновление сертификата:

   - В поле **Обновлять, когда до истечения срока действия осталось (сут)** укажите, за какое количество дней до истечения срока действия нужно обновлять сертификат.

   - Чтобы включить автоматическое обновление сертификатов, установите флажок **Автоматически перевыпускать сертификат, если это возможно**.

6. В блоке **Защита паролем** включите и настройте использование пароля при расшифровке сертификатов.

   > Защита паролем доступна только для мобильных сертификатов.

   a. Установите флажок **Запрашивать пароль при установке сертификата**.

   b. С помощью ползунка настройте максимальное количество символов в пароле для шифрования.

7. Нажмите на кнопку **OK**.

Интеграция с инфраструктурой открытых ключей

Интеграция приложения с инфраструктурой открытых ключей (Public Key Infrastructure, PKI) необходима для упрощения выписки доменных сертификатов пользователей. В результате интеграции выписка сертификатов происходит автоматически.

> Минимально поддерживаемая версия сервера PKI – Windows Server 2008.

Для интеграции с PKI необходимо настроить учетную запись. Учетная запись должна соответствовать следующим требованиям:

- быть доменным пользователем и администратором устройства, на котором установлен Сервер администрирования;

- иметь привилегию SeServiceLogonRight на устройстве с установленным Сервером администрирования.

Под настроенной учетной записью нужно хотя бы один раз выполнить вход на устройстве с установленным Сервером администрирования для того, чтобы создать постоянный профиль пользователя. В хранилище сертификатов этого пользователя, на устройстве с Сервером администрирования, необходимо установить сертификат агента регистрации, предоставленный администраторами домена.

Чтобы настроить интеграцию с инфраструктурой открытых ключей:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Сертификаты**.
2. В рабочей области нажмите на кнопку **Интегрировать с инфраструктурой открытых ключей**, чтобы открыть раздел **Интеграция с PKI** окна **Правила выпуска сертификатов**.

   Откроется раздел **Интеграция с PKI** окна **Правила выпуска сертификатов**.
3. Установите флажок **Интегрировать выписку сертификатов с PKI**.
4. В поле **Учетная запись** укажите имя учетной записи пользователя, которая будет использоваться для интеграции с инфраструктурой открытых ключей.
5. В поле **Пароль** укажите доменный пароль учетной записи.
6. В списке **Имя шаблона сертификата в системе PKI** выберите шаблон сертификата, который будет использоваться для выпуска сертификатов пользователям домена.

   Под указанной учетной записью в Kaspersky Security Center запускается специализированная служба. Эта служба отвечает за выпуск доменных сертификатов пользователей. Служба запускается, когда происходит загрузка списка шаблонов сертификатов по кнопке **Обновить список**, или при выпуске сертификата.
7. Нажмите на кнопку **OK**, чтобы сохранить параметры.

В результате интеграции выписка сертификатов происходит автоматически.

Включение поддержки Kerberos Constrained Delegation

Приложение поддерживает использование Kerberos Constrained Delegation.

Чтобы включить поддержку Kerberos Constrained Delegation:

1. В дереве консоли откройте папку **Управление мобильными устройствами**.
2. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
4. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.
5. В окне свойств Сервера iOS MDM выберите раздел **Параметры**.
6. В разделе **Параметры** установите флажок **Обеспечить совместимость с Kerberos constrained delegation**.
7. Нажмите на кнопку **OK**.

Добавление мобильных устройств iOS в список управляемых устройств

Чтобы добавить мобильное устройство iOS в список управляемых устройств, на устройство нужно доставить и установить общий сертификат. Общие сертификаты используются для идентификации мобильных устройств Сервером администрирования. Общий сертификат для мобильного устройства iOS доставляется в составе iOS MDM-профиля. После доставки и установки общего сертификата на мобильном устройстве, мобильное устройство отображается в списке управляемых устройств.

"Лаборатория Касперского" больше не поддерживает Kaspersky Safe Browser.

Вы можете добавить мобильные устройства пользователей в список управляемых устройств с помощью мастера подключения мобильного устройства.

Чтобы подключить iOS-устройство к Серверу администрирования, с использованием общего сертификата:

1. Запустите мастер подключения мобильного устройства одним из следующих способов:

   - В контекстом меню папки **Учетные записи пользователей**:

     1. В дереве консоли в папке **Дополнительно** выберите вложенную папку **Учетные записи пользователей**.

     2. В рабочей области папки **Учетные записи пользователей** выберите пользователей, группы безопасности или группы безопасности Active Directory пользователей, для которых вы хотите добавить мобильные устройства в список управляемых устройств.

     3. В контекстном меню учетной записи пользователя выберите пункт **Добавить мобильное устройство**.

        Запустится мастер подключения мобильного устройства.

   - Нажмите на кнопку **Добавить мобильное устройство** в рабочей области папки **Мобильные устройства**:

     1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

     2. В рабочей области вложенной папки **Мобильные устройства** нажмите на кнопку **Добавить мобильное устройство**.

        Запустится мастер подключения мобильного устройства.

2. В окне мастера **Операционная система** выберите тип операционной системы мобильного устройства **iOS**.

3. На странице **Выбор Сервера iOS MDM** выберите Сервер iOS MDM.

4. В рабочей области папки **Выбор пользователей, мобильными устройствами которых вы хотите управлять** выберите пользователей, группы безопасности или группы безопасности Active Directory пользователей, для которых вы хотите добавить мобильные устройства в список управляемых устройств.

Если вы запустили мастер выбрав пункт **Добавить мобильное устройство** в контекстном меню папки **Учетные записи пользователей**, этот шаг пропускается.

Если вы хотите добавить учетную запись пользователя в список, нажмите на кнопку **Добавить** и в открывшемся окне укажите параметры учетной записи пользователя. Если вы хотите изменить или просмотреть свойства учетной записи пользователя, выберите учетную запись пользователя из списка и нажмите на кнопку **Свойства**.

5. На странице мастера **Источник сертификата** укажите способ создания общего сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Вы можете задать общий сертификат одним из двух способов:

   - **Выписать сертификат средствами Сервера администрирования**

     Если выбран этот вариант, то iOS MDM-профиль будет подписан сертификатом, автоматически созданным Сервером администрирования.

     Этот вариант выбран по умолчанию.

   - **Указать файл сертификата**

     Укажите файл ранее созданного сертификата. Этот способ не доступен, если на предыдущем шаге было выбрано несколько пользователей.

6. На странице мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата с помощью SMS-сообщения или по электронной почте:

   - **Показать QR-код в мастере**

     При выборе этого варианта ссылка на инсталляционный пакет будет отображена на последнем шаге работы мастера подключения нового устройства.

     Этот вариант недоступен, если было выбрано несколько пользователей для подключения устройства.

   - **Отправить QR-код пользователю**

     При выборе этого варианта можно настроить параметры оповещения пользователя о подключении нового мобильного устройства.

     Можно выбрать тип адреса электронной почты, указать дополнительный адрес и отредактировать текст сообщения. Можно также выбрать тип телефона пользователя для отправки SMS-сообщения, указать дополнительный номер телефона и отредактировать текст отправляемого SMS-сообщения.

     Если не настроен SMTP-сервер, отправка сообщений электронной почты пользователям невозможна. Если не настроено SMS оповещение, отправка SMS-сообщений пользователям невозможна.

7. На странице мастера **Результат** нажмите на кнопку **Готово** для завершения работы мастера.

В результате iOS MDM-профиль автоматически публикуется на Веб-сервере Kaspersky Security Center. Пользователь мобильного устройства получит уведомление со ссылкой для загрузки iOS MDM-профиля с Веб-сервера. Пользователь самостоятельно переходит по полученной ссылке. После этого операционная система мобильного устройства запрашивает у пользователя согласие на установку iOS MDM-профиля. Чтобы iOS MDM-профиль загрузился на мобильное устройство, пользователь должен согласиться на установку iOS MDM-профиля. После загрузки iOS MDM-профиля и синхронизации с Сервером

администрирования мобильное устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Для перехода пользователем по полученной ссылке на Веб-сервере Kaspersky Security Center необходимо, чтобы с его мобильного устройства было доступно соединение с Сервером администрирования по порту 8061.

Добавление мобильных устройств Android в список управляемых устройств

Чтобы добавить мобильное устройство Android в список управляемых устройств, на устройство нужно доставить Kaspersky Endpoint Security для Android и установить общий сертификат. Общие сертификаты используются для идентификации мобильных устройств Сервером администрирования. После доставки и установки общего сертификата на мобильном устройстве, мобильное устройство отображается в списке управляемых устройств.

Вы можете добавить мобильные устройства пользователей в список управляемых устройств с помощью мастера подключения мобильного устройства. Мастер подключения нового мобильного устройства предоставляет два способа доставки и установки общего сертификата и Kaspersky Endpoint Security для Android:

- По ссылке на Google Play.
- По ссылке на Веб-сервер Kaspersky Security Center.

  Для установки используется инсталляционный пакет Kaspersky Endpoint Security для Android, сохраненный для распространения на Сервере администрирования.

Запуск мастера подключения мобильного устройства

Запустите мастер подключения мобильного устройства одним из следующих способов:

- В контекстом меню папки **Учетные записи пользователей**:

  1. В дереве консоли в папке **Дополнительно** выберите вложенную папку **Учетные записи пользователей**.
  2. В рабочей области папки **Учетные записи пользователей** выберите пользователей, группы безопасности или группы безопасности Active Directory пользователей, для которых вы хотите добавить мобильные устройства в список управляемых устройств.
  3. В контекстном меню учетной записи пользователя выберите пункт **Добавить мобильное устройство**.

     Запустится мастер подключения мобильного устройства.

- Нажмите на кнопку **Добавить мобильное устройство** в рабочей области папки **Мобильные устройства**:

  1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

  2. В рабочей области вложенной папки **Мобильные устройства** нажмите на кнопку **Добавить мобильное устройство**.

     Запустится мастер подключения мобильного устройства.

Добавление мобильного устройства Android с помощью ссылки Google Play

Чтобы установить Kaspersky Endpoint Security для Android и общий сертификат на мобильное устройство, используя ссылку на Google Play:

1. Запустится мастер подключения мобильного устройства.

2. В окне мастера **Операционная система** выберите тип операционной системы мобильного устройства **Android**.

3. На странице **Метод установки Kaspersky Endpoint Security для Android на устройства** в мастере выберите **Загрузить приложение из Google Play**.

4. На странице мастера **Выбор пользователей, мобильными устройствами которых вы хотите управлять** выберите пользователей, группы безопасности или группы безопасности Active Directory пользователей, для которых вы хотите добавить мобильные устройства в список управляемых устройств.

   > Этот шаг пропущен, если в контекстном меню папки **Учетные записи пользователей** выбран пункт **Добавить мобильное устройство**.

   Если вы хотите добавить учетную запись пользователя в список, нажмите на кнопку **Добавить** и в открывшемся окне укажите параметры учетной записи пользователя. Если вы хотите изменить или просмотреть свойства учетной записи пользователя, выберите учетную запись пользователя из списка и нажмите на кнопку **Свойства**.

5. На странице мастера **Источник сертификата** укажите способ создания общего сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Вы можете задать общий сертификат одним из двух способов:

   - **Выписать сертификат средствами Сервера администрирования**

     Если выбран этот вариант, сертификат автоматически создается средствами Сервера администрирования.

     Этот вариант выбран по умолчанию.

   - **Указать файл сертификата**

     Укажите файл ранее созданного сертификата. Этот способ не доступен, если на предыдущем шаге было выбрано несколько пользователей.

6. На странице мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата с помощью SMS-сообщения или по электронной почте:

   - **Показать QR-код в мастере**

     При выборе этого варианта ссылка на инсталляционный пакет будет отображена на последнем шаге работы мастера подключения нового устройства.

     > Этот вариант недоступен, если было выбрано несколько пользователей для подключения устройства.

   - **Отправить QR-код пользователю**

     При выборе этого варианта можно настроить параметры оповещения пользователя о подключении нового мобильного устройства.

     Можно выбрать тип адреса электронной почты, указать дополнительный адрес и отредактировать текст сообщения. Можно также выбрать тип телефона пользователя для отправки SMS-сообщения, указать дополнительный номер телефона и отредактировать текст отправляемого SMS-сообщения.

     Если не настроен SMTP-сервер, отправка сообщений электронной почты пользователям невозможна. Если не настроено SMS оповещение, отправка SMS-сообщений пользователям невозможна.

7. На странице мастера **Результат** нажмите на кнопку **Готово** для завершения работы мастера.

В результате работы мастера на мобильное устройство пользователя будет отправлена ссылка и QR-код для загрузки Kaspersky Endpoint Security для Android. Пользователь переходит по ссылке или сканирует QR-код. После этого операционная система мобильного устройства запрашивает у пользователя согласие на установку Kaspersky Endpoint Security для Android. После загрузки и установки Kaspersky Endpoint Security для Android мобильное устройство подключается к Серверу администрирования и загружает общий сертификат. После установки сертификата на мобильное устройство это устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Добавление мобильного устройства Android с помощью ссылки на Веб-сервер Kaspersky Security Center Web

> Для установки используется инсталляционный пакет Kaspersky Endpoint Security для Android, опубликованный на Сервере администрирования.

Чтобы установить Kaspersky Endpoint Security для Android и общий сертификат на мобильное устройство, используя ссылку на Веб-сервер:

1. Запустится мастер подключения мобильного устройства.

2. В окне мастера **Операционная система** выберите тип операционной системы мобильного устройства **Android**.

3. На странице **Метод установки Kaspersky Endpoint Security для Android на устройства** в мастере выберите **Загрузить установочный пакет приложения из Kaspersky Security Center**.

   В появившемся ниже поле выберите инсталляционный пакет или создайте новый инсталляционный пакет по кнопке **Новый**.

4. На странице мастера **Выбор пользователей, мобильными устройствами которых вы хотите управлять** выберите пользователей, группы безопасности или группы безопасности Active Directory пользователей, для которых вы хотите добавить мобильные устройства в список управляемых устройств.

   Этот шаг пропущен, если в контекстном меню папки **Учетные записи пользователей** выбран пункт **Добавить мобильное устройство**.

   Если вы хотите добавить учетную запись пользователя в список, нажмите на кнопку **Добавить** и в открывшемся окне укажите параметры учетной записи пользователя. Если вы хотите изменить или просмотреть свойства учетной записи пользователя, выберите учетную запись пользователя из списка и нажмите на кнопку **Свойства**.

5. На странице мастера **Источник сертификата** укажите способ создания общего сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Вы можете задать общий сертификат одним из двух способов:

   - **Выписать сертификат средствами Сервера администрирования**

     Если выбран этот вариант, сертификат автоматически создается средствами Сервера администрирования.

     Этот вариант выбран по умолчанию.

   - **Указать файл сертификата**

     Укажите файл ранее созданного сертификата. Этот способ не доступен, если на предыдущем шаге было выбрано несколько пользователей.

6. На странице мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата с помощью SMS-сообщения или по электронной почте:

   - **Показать QR-код в мастере**

     При выборе этого варианта ссылка на инсталляционный пакет будет отображена на последнем шаге работы мастера подключения нового устройства.

     Этот вариант недоступен, если было выбрано несколько пользователей для подключения устройства.

   - **Отправить QR-код пользователю**

     При выборе этого варианта можно настроить параметры оповещения пользователя о подключении нового мобильного устройства.

     Можно выбрать тип адреса электронной почты, указать дополнительный адрес и отредактировать текст сообщения. Можно также выбрать тип телефона пользователя для отправки SMS-сообщения, указать дополнительный номер телефона и отредактировать текст отправляемого SMS-сообщения.

     Если не настроен SMTP-сервер, отправка сообщений электронной почты пользователям невозможна. Если не настроено SMS оповещение, отправка SMS-сообщений пользователям невозможна.

7. На странице мастера **Результат** нажмите на кнопку **Готово** для завершения работы мастера.

В результате пакет мобильного приложения Kaspersky Endpoint Security для Android автоматически публикуется на Веб-сервере Kaspersky Security Center. Пакет мобильного приложения содержит приложение, параметры подключения мобильного устройства к Серверу администрирования и

сертификат. Пользователь мобильного устройства получит уведомление со ссылкой для загрузки пакета с Веб-сервера. Пользователь самостоятельно переходит по полученной ссылке. После этого операционная система устройства запрашивает у пользователя согласие на установку пакета мобильного приложения. Если пользователь соглашается, пакет загружается на мобильное устройство. После загрузки пакета и синхронизации с Сервером администрирования мобильное устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Управление iOS MDM-устройствами

В этом разделе описаны дополнительные возможности управления iOS MDM-устройствами с помощью Kaspersky Security Center. Для управления iOS MDM-устройствами приложение поддерживает следующие возможности:

- Централизованно настраивать параметры управляемых iOS MDM-устройств и ограничивать функции устройств с помощью конфигурационных профилей. Вы можете добавлять и изменять конфигурационные профили и устанавливать профили на мобильные устройства.
- Устанавливать приложения на мобильные устройства не через App Store с помощью provisioning-профилей. Например, с помощью provisioning-профилей можно устанавливать на мобильные устройства пользователей корпоративные приложения, разработанные внутри компании. Provisioning-профиль содержит информацию о приложении и мобильном устройстве.
- Устанавливать приложения на iOS MDM-устройство через App Store. Перед установкой приложения на iOS MDM-устройство приложение необходимо добавить на Сервер iOS MDM.

Каждые 24 часа всем подключенным iOS MDM-устройствам отправляется PUSH-нотификация для синхронизации данных с Сервером iOS MDM.

Информацию о конфигурационном профиле и provisioning–профиле, а также о приложениях, установленных на iOS MDM-устройстве, можно просмотреть в окне свойств устройства.

Подписание iOS MDM-профиля сертификатом

Вы можете подписать iOS MDM-профиль сертификатом. Вы можете использовать сертификат, выписанный вами самостоятельно, или получить сертификат от доверенного центра сертификации.

iOS-устройства отображают отказ от ответственности для неподписанных профилей и предлагают пользователю доверять подписывающему лицу при установке профиля.

Чтобы подписать iOS MDM-профиль сертификатом:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.
2. В контекстном меню папки **Мобильные устройства** выберите пункт **Свойства**.
3. В окне свойств папки выберите раздел **Параметры подключения iOS-устройств**.
4. Нажмите на кнопку **Обзор** под полем **Выбрать файл сертификата**.

   Откроется окно **Сертификат**.

5. В поле **Тип сертификата** выберите открытый или закрытый тип сертификата:

   - Если выбрано значение **Контейнер PKCS#12**, укажите файл сертификата и пароль.
   - Если выбрано значение **X.509-сертификат**:

     a. укажите файл закрытого ключа (файл с расширением prk или pem);

     b. укажите пароль закрытого ключа;

     c. укажите файл открытого ключа (файл с расширением cer).

6. Нажмите на кнопку **OK**.

iOS MDM-профиль подписан сертификатом.

Добавление конфигурационного профиля

Чтобы создать конфигурационный профиль, вы можете использовать приложение Apple Configurator 2, которое доступно на веб-сайте Apple Inc. Приложение Apple Configurator 2 работает только на устройствах под управлением macOS; если у вас нет таких устройств, вы можете использовать iPhone Configuration Utility на устройстве с установленной Консолью администрирования. Apple Inc. больше не поддерживает iPhone Configuration Utility.

Чтобы создать конфигурационный профиль с помощью iPhone Configuration Utility и добавить его на Сервер iOS MDM:

1. В дереве консоли выберите папку **Управление мобильными устройствами**.
2. В рабочей области папки **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
4. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера мобильных устройств.

5. В окне свойств Сервера iOS MDM выберите раздел **Конфигурационные профили**.
6. В разделе **Конфигурационные профили** нажмите на кнопку **Создать**.

   Откроется окно **Новый конфигурационный профиль**.

7. В окне **Новый конфигурационный профиль** укажите название профиля и идентификатор профиля.

   Идентификатор конфигурационного профиля должен быть уникальным, значение идентификатора следует задавать в формате Reverse-DNS, например, *com.companyname.identifier*.

8. Нажмите на кнопку **OK**.

   Запустится приложение iPhone Configuration Utility, если оно установлено.

9. Выполните настройку параметров профиля в приложении iPhone Configuration Utility.

   Описание параметров профиля и инструкции по его настройке приведены в документации для приложения iPhone Configuration Utility.

После настройки параметров профиля в приложении iPhone Configuration Utility, новый конфигурационный профиль отображается в разделе **Конфигурационные профили** в окне свойств Сервера iOS MDM.

По кнопке **Изменить** конфигурационный профиль можно отредактировать.

По кнопке **Импортировать** можно загрузить конфигурационный профиль в приложение.

По кнопке **Экспортировать** конфигурационный профиль можно сохранить в файле.

Созданный профиль требуется установить на iOS MDM-устройства.

Установка конфигурационного профиля на устройство

Чтобы установить конфигурационный профиль на мобильное устройство:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте iOS MDM-устройства по протоколу управления *iOS MDM*.

3. Выберите мобильное устройство пользователя, на которое нужно установить конфигурационный профиль

   Вы можете выбрать несколько мобильных устройств, чтобы установить на них профиль одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Установить профиль** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню мобильного устройства пункт **Все команды**, затем **Установить профиль**.

   В результате откроется окно **Выбор профилей** со списком профилей. Выберите в списке профиль, который нужно установить на мобильное устройство. Вы можете выбрать и установить на мобильное устройство несколько профилей одновременно. Чтобы выбрать диапазон профилей, используйте клавишу **SHIFT**. Для объединения отдельных профилей в группу используйте клавишу **CTRL**.

6. Нажмите на кнопку **OK**, чтобы отправить команду на мобильное устройство.

   В результате выполнения команды выбранный конфигурационный профиль будет установлен на мобильное устройство пользователя. В случае успешного выполнения команды текущий статус команды в журнале команд примет значение *Выполнено*.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

   По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

7. Нажмите на кнопку **OK**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Вы можете просмотреть профиль, который вы установили, и удалить его, если необходимо.

Удаление конфигурационного профиля с устройства

Чтобы удалить конфигурационный профиль с мобильного устройства:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте iOS MDM-устройства по ссылке **iOS MDM**.

3. Выберите мобильное устройство пользователя, с которого нужно удалить конфигурационный профиль.

   Вы можете выбрать несколько мобильных устройств, чтобы удалить с них профиль одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Удалить профиль** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню устройства пункт **Все команды**, затем **Удалить профиль**.

   В результате откроется окно **Удаление профилей** со списком профилей.

6. Выберите в списке профиль, который нужно удалить с мобильного устройства. Вы можете выбрать и удалить с мобильного устройства несколько профилей одновременно. Чтобы выбрать диапазон профилей, используйте клавишу **SHIFT**. Для объединения отдельных профилей в группу используйте клавишу **CTRL**.

7. Нажмите на кнопку **OK**, чтобы отправить команду на мобильное устройство.

   В результате выполнения команды выбранный конфигурационный профиль будет удален с мобильного устройства пользователя. В случае успешного выполнения команды текущий статус команды примет значение *Завершена*.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

   По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

   В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

8. Нажмите на кнопку **OK**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Добавление нового устройства посредством публикации ссылки на профиль

В Консоли администрирования с помощью мастера установки сертификатов администратор создает новый iOS MDM-профиль. В результате работы мастера будут выполнены следующие действия:

- iOS MDM-профиль автоматически опубликуется на Веб-сервере.
- Пользователю будет отправлена ссылка на iOS MDM-профиль в SMS-сообщении или по электронной почте. После получения ссылки пользователь установит iOS MDM-профиль на мобильном устройстве.
- В результате мобильное устройство будет подключено к Серверу iOS MDM.

В связи с введенным компанией Apple ужесточением политики безопасности, для подключения мобильного устройства с операционной системой iOS 11 к Серверу администрирования с настроенной интеграцией с Public Key Infrastructure (PKI) необходимо настроить протоколы версий TLS 1.1 и TLS 1.2.

Добавление нового устройства посредством установки профиля администратором

Чтобы подключить мобильное устройство к Серверу iOS MDM с помощью установки iOS MDM-профиля на мобильное устройство, администратор должен выполнить следующие действия:

1. В Консоли администрирования откройте мастер установки сертификата.
2. Создать новый iOS MDM-профиль, установив в окне мастера создания профиля флажок **Показать сертификат после завершения работы мастера**.
3. Сохранить iOS MDM-профиль.
4. Установить iOS MDM-профиль на мобильное устройство пользователя с помощью утилиты Apple Configurator.

В результате мобильное устройство будет подключено к Серверу iOS MDM.

В связи с введенным компанией Apple ужесточением политики безопасности, для подключения мобильного устройства с операционной системой iOS 11 к Серверу администрирования с настроенной интеграцией с Public Key Infrastructure (PKI) необходимо настроить протоколы версий TLS 1.1 и TLS 1.2.

Добавление provisioning-профиля

Чтобы добавить provisioning-профиль на Сервер iOS MDM:

1. В дереве консоли откройте папку **Управление мобильными устройствами**.
2. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.

4. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера мобильных устройств.

5. В окне свойств **Сервера iOS MDM** перейдите в раздел **Provisioning-профили**.

6. В разделе **Provisioning-профили** нажмите на кнопку **Импортировать** и укажите путь к файлу provisioning-профиля.

Профиль будет добавлен в параметры Сервера iOS MDM.

По кнопке **Экспортировать** provisioning-профиль можно сохранить в файле.

Вы можете установить provisioning-профиль, который вы импортировали, на iOS MDM-устройства.

Установка provisioning-профиля на устройство

Чтобы установить provisioning-профиль на мобильное устройство:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте iOS MDM-устройства по протоколу управления *iOS MDM*.

3. Выберите мобильное устройство пользователя, на которое нужно установить provisioning-профиль.

   Вы можете выбрать несколько мобильных устройств, чтобы установить на них provisioning-профиль одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Установить provisioning-профиль** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню мобильного устройства пункт **Все команды**, затем **Установить provisioning-профиль**.

   В результате откроется окно **Выбор provisioning-профилей** со списком provisioning-профилей. Выберите в списке provisioning-профиль, который нужно установить на мобильное устройство. Вы можете выбрать и установить на мобильное устройство несколько provisioning-профилей одновременно. Чтобы выбрать диапазон provisioning-профилей, используйте клавишу **SHIFT**. Для объединения отдельных provisioning-профилей в группу используйте клавишу **CTRL**.

6. Нажмите на кнопку **OK**, чтобы отправить команду на мобильное устройство.

   В результате выполнения команды выбранный provisioning-профиль будет установлен на мобильное устройство пользователя. В случае успешного выполнения команды текущий статус команды в журнале команд принимает значение *Завершена*.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

   По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

7. Нажмите на кнопку **OK**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Вы можете просмотреть профиль, который вы установили, и удалить его, если необходимо.

Удаление provisioning-профиля с устройства

Чтобы удалить provisioning-профиль с мобильного устройства:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте iOS MDM-устройства по протоколу управления *iOS MDM*.

3. Выберите мобильное устройство пользователя, с которого нужно удалить provisioning-профиль.

   Вы можете выбрать несколько мобильных устройств, чтобы удалить с них provisioning-профиль одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Удалить provisioning-профиль** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню устройства пункт **Все команды**, затем **Удалить provisioning-профиль**.

   В результате откроется окно **Удаление provisioning-профилей** со списком профилей.

6. Выберите в списке provisioning-профиль, который нужно удалить с мобильного устройства. Вы можете выбрать и удалить с мобильного устройства несколько provisioning-профилей одновременно. Чтобы выбрать диапазон provisioning-профилей, используйте клавишу **SHIFT**. Для объединения отдельных provisioning-профилей в группу используйте клавишу **CTRL**.

7. Нажмите на кнопку **OK**, чтобы отправить команду на мобильное устройство.

   В результате выполнения команды выбранный provisioning-профиль будет удален с мобильного устройства пользователя. Приложения, связанные с удаленным provisioning-профилем, не будут работать. В случае успешного выполнения команды текущий статус команды примет значение *Завершена*.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

   По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

   В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

8. Нажмите на кнопку **OK**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Добавление управляемого приложения

Перед установкой приложения на iOS MDM-устройство приложение необходимо добавить на Сервер iOS MDM. Приложение является управляемым, если оно было установлено на устройство с помощью Kaspersky Security Center. Управляемым приложением можно дистанционно управлять средствами Kaspersky Security Center.

Чтобы добавить управляемое приложение на Сервер iOS MDM:

1. В дереве консоли откройте папку **Управление мобильными устройствами**.
2. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
4. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера iOS MDM.
5. В окне свойств Сервера iOS MDM выберите раздел **Управляемые приложения**.
6. В разделе **Управляемые приложения** нажмите на кнопку **Добавить**.

   Откроется окно **Добавление приложения**.
7. В окне **Добавление приложения** в поле **Название приложения** укажите название добавляемого приложения.
8. В поле **Apple ID приложения или ссылка на манифест-файл** укажите Apple ID добавляемого приложения или ссылку на манифест-файл, по которой можно загрузить приложение.
9. Если вы хотите, чтобы при удалении iOS MDM-профиля одновременно с профилем с мобильного устройства пользователя было удалено и управляемое приложение, установите флажок **Удалять вместе с iOS MDM-профилем**.
10. Если вы хотите запретить резервное копирование данных приложения с помощью iTunes, установите флажок **Запретить создавать резервные копии данных**.
11. Нажмите на кнопку **OK**.

Добавленное приложение отображается в разделе **Управляемые приложения** окна свойств Сервера iOS MDM.

Установка приложения на мобильное устройство

Чтобы установить приложение на мобильное устройство iOS MDM:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.
2. Выберите iOS MDM-устройство, на которое нужно установить приложение.

   Вы можете выбрать несколько мобильных устройств, чтобы установить на них приложение одновременно.

3. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

4. В окне **Команды для управления мобильным устройством** перейдите в раздел **Установить приложение** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню мобильного устройства пункт **Все команды**, затем **Установить приложение**.

   В результате откроется окно **Выбор приложений** со списком профилей. Выберите в списке приложение, которое нужно установить на мобильное устройство. Вы можете выбрать и установить на мобильное устройство несколько приложений одновременно. Чтобы выбрать диапазон приложений, используйте клавишу **SHIFT**. Для объединения отдельных приложений в группу используйте клавишу **CTRL**.

5. Нажмите на кнопку **OK**, чтобы отправить команду на мобильное устройство.

   В результате выполнения команды выбранное приложение будет установлено на мобильное устройство пользователя. В случае успешного выполнения команды текущий статус команды в журнале команд принимает значение *Завершена*.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз. По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

   В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

6. Нажмите на кнопку **OK**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Информация об установленном приложении отображается в свойствах мобильного устройства iOS MDM. Вы можете удалить приложение с мобильного устройства с помощью журнала команд или из контекстного меню мобильного устройства.

Удаление приложения с устройства

Чтобы удалить приложение с мобильного устройства:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте iOS MDM-устройства по протоколу управления *iOS MDM*.

3. Выберите мобильное устройство пользователя, с которого нужно удалить приложение.

   Вы можете выбрать несколько мобильных устройств, чтобы удалить с них приложение одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Удалить приложение** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню мобильного устройства пункт **Все команды**, затем **Удалить приложение**.

   В результате откроется окно **Удаление приложений** со списком приложений.

6. Выберите в списке приложение, которое нужно удалить с мобильного устройства. Вы можете выбрать и удалить с устройства несколько приложений одновременно. Чтобы выбрать диапазон приложений, используйте клавишу **SHIFT**. Для объединения отдельных приложений в группу используйте клавишу **CTRL**.

7. Нажмите на кнопку **OK**, чтобы отправить команду на мобильное устройство.

   В результате выполнения команды выбранное приложение будет удалено с мобильного устройства пользователя. В случае успешного выполнения команды текущий статус команды примет значение *Завершена*.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

   По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

   В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

8. Нажмите на кнопку **OK**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Настройка параметров роуминга на мобильном устройстве iOS MDM

Чтобы настроить параметры роуминга:

1. В дереве консоли откройте папку **Управление мобильными устройствами**.
2. В папке **Управление мобильными устройствами** выберите подпапку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

3. Выберите iOS MDM-устройство пользователя, для которого нужно настроить роуминг.

   Вы можете выбрать несколько мобильных устройств, чтобы настроить для них роуминг одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.
5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Настроить параметры роуминга** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню устройства пункт **Все команды → Настроить параметры роуминга**.

6. В окне **Параметры роуминга** укажите нужные вам параметры:

   - **Включить роуминг данных**

     Если флажок установлен, на мобильном устройстве iOS MDM включен роуминг данных. Пользователь iOS MDM-устройства может пользоваться интернетом в роуминге.

     По умолчанию флажок снят.

Параметры роуминга настроены для выбранных устройств.

Просмотр информации о iOS MDM-устройстве

Чтобы просмотреть информацию о iOS MDM-устройстве:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте iOS MDM-устройства по ссылке **iOS MDM**.

3. Выберите мобильное устройство, информацию о котором нужно просмотреть.

4. В контекстном меню мобильного устройства выберите пункт **Свойства**.

   В результате откроется окно свойств iOS MDM-устройства.

В окне свойств мобильного устройства отображается информация о подключенном iOS MDM-устройстве.

Отключение iOS MDM-устройства от управления

Чтобы отключить iOS MDM-устройство от Сервера iOS MDM:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте iOS MDM-устройства по ссылке **iOS MDM**.

3. Выберите мобильное устройство, которое необходимо отключить.

4. В контекстном меню мобильного устройства выберите пункт **Удалить**.

   В результате iOS MDM-устройство будет отмечено в списке на удаление. Мобильное устройство будет автоматически удалено из списка управляемых устройств после его удаления из базы данных Сервера iOS MDM. Удаление мобильного устройства из базы данных Сервера iOS MDM происходит в течение одной минуты.

В результате отключения iOS MDM-устройства от управления с мобильного устройства будут удалены все установленные конфигурационные профили, iOS MDM-профиль и приложения, для которых был выбран параметр **Удалять вместе с iOS MDM-профилем**.

Отправка команд на устройство

Чтобы отправить команду на iOS MDM-устройство:

1. В Консоли администрирования разверните узел **Управление мобильными устройствами**.

2. Выберите папку **Мобильные устройства**.

3. В папке **Мобильные устройства** выбрать мобильное устройство, на которое необходимо отправить команды.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

5. Во всплывающем списке выберите необходимую команду для отправки на мобильное устройство.

Проверка статуса исполнения отправленных команд

Чтобы проверить статус выполнения команды, отправленной на мобильное устройство:

1. В Консоли администрирования разверните узел **Управление мобильными устройствами**.
2. Выберите папку **Мобильные устройства**.
3. В папке **Мобильные устройства** выбрать мобильное устройство, на котором необходимо проверить статус выполнения отправленных команд.
4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

Управление KES-устройствами

В Kaspersky Security Center вы можете управлять KES-устройствами следующими способами:

- централизованно управлять KES-устройствами с помощью команд;
- просматривать информацию о параметрах управления KES-устройствами;
- устанавливать приложения с помощью пакетов мобильных приложений;
- отключать KES-устройства от управления.

Создание пакета мобильных приложений для KES-устройств

Для создания пакета мобильных приложений для KES-устройств необходима лицензия Kaspersky Endpoint Security для Android.

Чтобы создать пакет мобильных приложений:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.

   Папка **Удаленная установка** по умолчанию вложена в папку **Дополнительно**.
2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите значение **Управлять пакетами мобильных приложений**.
3. В окне **Управление пакетами мобильных приложений** нажмите на кнопку **Новый**.
4. Запустится мастер создания инсталляционного пакета. Следуйте далее указаниям мастера.

Созданный пакет мобильных приложений отобразится в окне **Управление пакетами мобильных приложений**.

Включение проверки подлинности на основе сертификатов KES-устройств

Чтобы включить проверку подлинности на основе сертификатов KES-устройства:

1. Откройте системный реестр клиентского устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:
   - для 32-разрядной системы:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - для 64-разрядной системы:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. Создайте ключ с именем LP_MobileMustUseTwoWayAuthOnPort13292.
4. Укажите тип ключа REG_DWORD.
5. Установите значение ключа 1.
6. Перезапустите службу Сервера администрирования.

В результате обязательная проверка подлинности на основе сертификатов KES-устройства с использованием общего сертификата будет включена после запуска службы Сервера администрирования.

При первом подключении KES-устройства к Серверу администрирования наличие сертификата не обязательно.

По умолчанию проверка подлинности на основе сертификатов KES-устройств отключена.

Просмотр информации о KES-устройстве

Чтобы просмотреть информацию о KES-устройстве:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.
   В рабочей области папки отображается список управляемых мобильных устройств.
2. В рабочей области отфильтруйте KES-устройства по протоколу управления *KES*.
3. Выберите мобильное устройство, информацию о котором нужно просмотреть.
4. В контекстном меню мобильного устройства выберите пункт **Свойства**.

В результате откроется окно свойств KES-устройства.

В окне свойств мобильного устройства отображается информация о подключенном KES-устройстве.

Отключение KES-устройства от управления

Чтобы отключить KES-устройство от управления, пользователь должен удалить Агент администрирования с мобильного устройства. После удаления пользователем Агента администрирования информация о мобильном устройстве удаляется из базы данных Сервера администрирования и администратор может удалить мобильное устройство из списка управляемых устройств.

Чтобы удалить KES-устройство из списка управляемых устройств:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте KES-устройства по протоколу управления *KES*.

3. Выберите мобильное устройство, которое необходимо отключить от управления.

4. В контекстном меню мобильного устройства выберите пункт **Удалить**.

В результате мобильное устройство будет удалено из списка управляемых устройств.

Если Kaspersky Endpoint Security для Android не удален с мобильного устройства, то после синхронизации с Сервером администрирования мобильное устройство снова появится в списке управляемых устройств.

Шифрование и защита данных

Шифрование данных снижает риски непреднамеренной утечки информации в случае кражи/утери портативного устройства, съемного диска или жесткого диска, или при доступе к данным неавторизованных пользователей и приложений.

Шифрование реализовано в приложении Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security для Windows позволяет шифровать файлы, хранящиеся на локальных дисках устройств и съемных дисках, съемные диски и жесткие диски целиком.

Настройка правил шифрования выполняется с помощью Kaspersky Security Center через определение политик. Шифрование и расшифровка по заданным правилам выполняются при применении политики.

Доступность функциональности управления шифрованием определяется параметрами пользовательского интерфейса.

Администратор может выполнять следующие действия:

- настраивать и выполнять шифрование или расшифровку файлов на локальных дисках устройства;
- настраивать и выполнять шифрование файлов на съемных дисках;
- формировать правила доступа приложений к зашифрованным файлам;
- создавать и передавать пользователю файл ключа доступа к зашифрованным файлам, если на устройстве пользователя ограничена функциональность шифрования файлов;

- настраивать и выполнять шифрование жестких дисков;
- управлять доступом пользователей к зашифрованным жестким дискам и съемным дискам (управлять учетными записями агента аутентификации, формировать и передавать пользователям блоки ответа на запрос о восстановлении имени и пароля учетной записи и ключи доступа к зашифрованным устройствам);
- просматривать статусы шифрования и отчеты о шифровании файлов.

Эти операции выполняются средствами приложения Kaspersky Endpoint Security для Windows. Подробные инструкции по выполнению операций и описание особенностей шифрования приведены в справке Kaspersky Endpoint Security для Windows.

Kaspersky Security Center поддерживает функционал управления шифрованием для устройств с операционными системами macOS. Настройка шифрования выполняется средствами приложения Kaspersky Endpoint Security для Mac для тех версий приложений, которые поддерживают шифрование. Подробные инструкции по выполнению операций и описание особенностей шифрования приведены в *Руководстве администратора Kaspersky Endpoint Security для Mac*.

Просмотр списка зашифрованных устройств

Чтобы просмотреть список устройств, информация на которых была зашифрована:

1. В дереве консоли Сервера администрирования выберите папку **Шифрование и защита данных**.
2. Перейдите к списку зашифрованных устройств одним из следующих способов:
   - По ссылке **Перейти к списку зашифрованных жестких дисков** перейдите в раздел **Управление зашифрованными жесткими дисками**.
   - Выберите в дереве консоли папку **Зашифрованные жесткие диски**.

В результате в рабочей области будет представлена информация об имеющихся в сети устройствах, на которых есть зашифрованные файлы, и устройствах, зашифрованных на уровне дисков. После того, как информация на устройстве будет расшифрована, устройство будет автоматически удалено из списка.

Вы можете сортировать информацию в списке устройств по возрастанию или убыванию данных любой из граф.

Наличие или отсутствие папки **Шифрование и защита данных** в дереве консоли определяется параметрами пользовательского интерфейса.

Просмотр списка событий шифрования

В процессе выполнения задач шифрования или расшифровки данных на устройствах Kaspersky Endpoint Security для Windows отправляет в Kaspersky Security Center информацию о возникающих событиях следующих типов:

- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за нехватки места на диске;
- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за проблем с лицензией;
- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за отсутствия прав доступа;
- приложению запрещен доступ к зашифрованному файлу;
- неизвестные ошибки.

Чтобы просмотреть список событий, возникших при шифровании данных на устройствах:

1. В дереве консоли Сервера администрирования выберите папку **Шифрование и защита данных**.
2. Перейдите к списку событий, возникших при шифровании, одним из следующих способов:
   - По ссылке **Перейти к списку ошибок** перейдите в раздел **Ошибки шифрования данных**.
   - Выберите в дереве консоли папку **Зашифрованные жесткие диски**.

В результате в рабочей области будет представлена информация о проблемах, возникших при шифровании данных на устройствах.

Вы можете выполнять следующие действия со списком событий шифрования:

- сортировать записи по возрастанию или убыванию данных в любой из граф;
- выполнять быстрый поиск по записям (по текстовому совпадению с подстрокой в любом поле списка);
- экспортировать сформированный список событий в текстовый файл.

Наличие или отсутствие папки **Шифрование и защита данных** в дереве консоли определяется параметрами пользовательского интерфейса.

Экспорт списка событий шифрования в текстовый файл

Чтобы экспортировать список событий шифрования в текстовый файл:

1. Сформируйте список событий шифрования.
2. В контекстном меню списка событий выберите пункт **Экспортировать список**.

   Откроется окно **Экспорт списка**.
3. В окне **Экспорт списка** укажите имя текстового файла со списком событий, выберите папку, в которую он будет сохранен, и нажмите на кнопку **Сохранить**.

   Список событий шифрования будет сохранен в указанный файл.

Формирование и просмотр отчетов о шифровании

Вы можете формировать следующие отчеты:

- Отчет о статусе шифрования управляемых устройств. В этом отчете представлены сведения о шифровании данных различных управляемых устройств. Например, в отчете показано количество устройств, к которым применяется политика с настроенными правилами шифрования. Также можно узнать, например, сколько устройств нужно перезагрузить. Отчет также содержит информацию о технологии и алгоритме шифрования для каждого устройства.
- Отчет о статусе шифрования запоминающих устройств. Этот отчет содержит похожую информацию, что и отчет о состоянии шифрования управляемых устройств, но предоставляет данные только для запоминающих устройств и съемных дисков.
- Отчет о правах доступа к зашифрованным дискам. Этот отчет показывает, какие учетные записи пользователей имеют доступ к зашифрованным жестким дискам.
- Отчет об ошибках шифрования файлов. Отчет содержит информацию об ошибках, которые возникли при выполнении задач шифрования или расшифровки данных на устройствах.
- Отчет о блокировании доступа к зашифрованным файлам. Отчет содержит информацию о блокировке доступа приложений к зашифрованным файлам. Этот отчет полезен, если неавторизованный пользователь или приложение пытается получить доступ к зашифрованным файлам или жестким дискам.

Чтобы сгенерировать отчет шифрования устройств:

1. В дереве консоли выберите папку **Шифрование и защита данных**.
2. Выполните одно из следующих действий:

   - Чтобы сгенерировать отчет о статусе шифрования управляемых устройств, перейдите по ссылке **Отчет о статусе шифрования запоминающих устройств**.

     Если отчет не был настроен ранее, запустится мастер создания шаблонов отчетов. Следуйте далее указаниям мастера.

   - Чтобы сформировать отчет о статусе шифрования запоминающих устройств, в дереве консоли выберите подпапку **Зашифрованные жесткие диски** и нажмите на кнопку **Отчет о статусе шифрования запоминающих устройств**.

   Запустится процесс формирования отчета. Отчет отображается в рабочей области узла **Сервер администрирования** на вкладке **Отчеты**.

Чтобы сформировать отчет о правах доступа к зашифрованным устройствам:

1. В дереве консоли выберите папку **Шифрование и защита данных**.
2. Выполните одно из следующих действий:

   - По ссылке **Отчет о правах доступа к зашифрованным дискам** в блоке **Управление зашифрованными жесткими дисками** запустите мастер создания шаблона отчета.

   - Выберите вложенную папку **Зашифрованные жесткие диски**, а затем запустите мастер создания шаблона отчета, нажав на кнопку **Отчет о правах доступа к зашифрованным дискам**.

3. Следуйте шагам мастера создания шаблона отчета.

   Запустится процесс формирования отчета. Отчет отображается в рабочей области узла **Сервер администрирования** на вкладке **Отчеты**.

Чтобы сгенерировать отчет об ошибках шифрования файлов:

1. В дереве консоли выберите папку **Шифрование и защита данных**.
2. Выполните одно из следующих действий:

   - По ссылке **Просмотреть отчет об ошибках шифрования файлов** в блоке управления **Ошибки шифрования данных** запустите мастер создания шаблона отчета.

   - Выберите вложенную папку **События шифрования**, а затем по ссылке **Отчет об ошибках шифрования файлов** запустите мастер создания шаблона отчета.

3. Следуйте шагам мастера создания шаблона отчета.

   Запустится процесс формирования отчета. Отчет отображается в рабочей области узла **Сервер администрирования** на вкладке **Отчеты**.

Чтобы сгенерировать отчет о статусе шифрования управляемых устройств:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. По кнопке **Новый шаблон отчета** запустите мастер создания шаблона отчета.
4. Следуйте указаниям мастера создания шаблона отчета. В окне **Выбор типа шаблона отчета** в разделе **Другое** выберите **Отчет о статусе шифрования управляемых устройств**.

   После завершения работы мастера создания шаблона отчета в узле Сервер администрирования на вкладке **Отчеты** появится новый шаблон отчета.
5. В узле нужного вам Сервера администрирования на вкладке **Отчеты** выберите шаблон отчета, созданный на предыдущих шагах инструкции.

Запустится процесс формирования отчета. Отчет отображается в рабочей области узла **Сервер администрирования** на вкладке **Отчеты**.

Информацию о соответствии статусов шифрования устройств и съемных дисков политике шифрования также можно просматривать в информационных панелях на вкладке **Статистика** узла Сервер администрирования.

Чтобы сгенерировать отчет о блокировании доступа к зашифрованным файлам:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите вкладку **Отчеты**.
3. По кнопке **Новый шаблон отчета** запустите мастер создания шаблона отчета.
4. Следуйте указаниям мастера создания шаблона отчета. В окне **Выбор типа шаблона отчета** в разделе **Другое** выберите **Отчет о блокировании доступа к зашифрованным файлам**.

   После завершения работы мастера создания шаблона отчета в узле **Сервер администрирования** на вкладке **Отчеты** появится новый шаблон отчета.
5. В узле **Сервер администрирования** на вкладке **Отчеты** выберите шаблон отчета, созданный на предыдущих шагах инструкции.

Запустится процесс формирования отчета. Отчет отображается в рабочей области узла **Сервер администрирования** на вкладке **Отчеты**.

Передача ключей шифрования между Серверами администрирования

Если на управляемом устройстве включена функция шифрования данных, ключ шифрования хранится на Сервере администрирования. Ключ шифрования используется для доступа к зашифрованным данным и для управления политикой шифрования.

Ключ шифрования должен быть передан на другой Сервер администрирования в следующих случаях:

- Вы переконфигурировали Агент администрирования на управляемом устройстве, чтобы назначить устройство другому Серверу администрирования. Если это устройство содержит зашифрованные данные, ключ шифрования должен быть передан на целевой Сервер администрирования. В противном случае не удастся расшифровать данные.

- Вы зашифровали съемный диск, подключенный к устройству D1, которым управляет Сервер администрирования S1, а затем подключаете этот съемный диск к устройству D2, управляемому Сервером администрирования S2. Для доступа к данным на съемном диске ключ шифрования должен быть передан с Сервера администрирования S1 на Сервер администрирования S2.

- Вы зашифровали файл на устройстве D1, управляемом Сервером администрирования S1, и затем пытаетесь получить доступ к файлу на устройстве D2, управляемом Сервером администрирования S2. Для доступа к файлу ключ шифрования должен быть передан с Сервера администрирования S1 на Сервер администрирования S2.

Ключи шифрования можно передавать следующими способами:

- Автоматически, включив параметр **Использовать иерархию Серверов администрирования для получения ключей шифрования** в свойствах двух Серверов администрирования, между которыми должен передаваться ключ шифрования. Если этот параметр выключен для одного из Серверов администрирования, автоматическая передача ключей шифрования невозможна.

  При включении параметра **Использовать иерархию Серверов администрирования для получения ключей шифрования** в свойствах Сервера администрирования, Сервер администрирования отправляет ключи шифрования на главный Сервер администрирования (если он существует) на один уровень иерархии выше.

  Когда вы пытаетесь получить доступ к зашифрованным данным, Сервер администрирования сначала ищет ключ шифрования в своем хранилище. Если включен параметр **Использовать иерархию Серверов администрирования для получения ключей шифрования**, а требуемый ключ шифрования отсутствует в хранилище, Сервер администрирования дополнительно отправляет запрос на главный Сервер администрирования (если он существует), чтобы получить требуемый ключ шифрования. Запрос отправляется на все главные Серверы администрирования, вплоть до Сервера на самом верхнем уровне иерархии.

Параметр **Использовать иерархию Серверов администрирования для получения ключей шифрования** недоступен в интерфейсе Web Console. Если у вас нет доступа к Консоли администрирования на основе MMC, используйте главный Сервер администрирования для управления зашифрованными устройствами.

- Вручную от одного Сервера администрирования другому путем экспорта и импорта файла, содержащего ключи шифрования.

  Экспорт и импорт ключей шифрования – это действия, включенные в функционал управления ключами шифрования. Чтобы выполнить эти действия, настройте права доступа к функции для пользователей Kaspersky Security Center следующим образом:

  - Предоставить право **Чтение** к функции Управление ключами шифрования для пользователя, который экспортирует ключи шифрования с подчиненного Сервера администрирования.

  - Предоставить право **Запись** к функции Управление ключами шифрования для пользователя, импортирующего ключи шифрования на требуемый Сервер администрирования.

Чтобы включить автоматическую передачу ключей шифрования между Серверами администрирования в иерархии:

1. В дереве консоли выберите Сервер администрирования, для которого нужно включить автоматическую передачу ключей шифрования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств выберите раздел **Алгоритм шифрования**.
4. Включите параметр **Использовать иерархию Серверов администрирования для получения ключей шифрования**.
5. Нажмите на кнопку **ОК**, чтобы применить изменения.

Ключи шифрования будут переданы на главный Сервер администрирования (если он существует) при следующей синхронизации (пакете пульса). Этот Сервер администрирования также предоставляет по запросу ключ шифрования от своего хранилища подчиненному Серверу администрирования.

Чтобы передать ключи шифрования между Серверами администрирования вручную:

1. В дереве консоли Сервера администрирования выберите подчиненный Сервер администрирования, с которого требуется передать ключи шифрования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств выберите раздел **Алгоритм шифрования**.
4. Нажмите на кнопку **Экспортировать ключи шифрования с Сервера администрирования**.

   Убедитесь, что пользователю, который экспортирует ключи шифрования с Сервера, предоставлено право **Чтение** к функции Управления ключами шифрования.
5. В окне **Экспорт ключей шифрования**:
   - Нажмите на кнопку **Обзор**, а затем укажите, куда сохранить файл.
   - Укажите пароль, чтобы защитить файл от несанкционированного доступа.

     Запомните пароль. Утерянный пароль не может быть восстановлен. Если пароль утерян, необходимо повторить процедуру экспорта. Поэтому запишите пароль и держите его под рукой.
6. Передайте файл на другой Сервер администрирования, например, с помощью папки общего доступа или съемного диска.
7. Убедитесь, что на целевом Сервере администрирования запущена Консоль администрирования Kaspersky Security Center.
8. В дереве консоли Сервера администрирования выберите целевой Сервер администрирования, куда требуется передать ключи шифрования.
9. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
10. В окне свойств выберите раздел **Алгоритм шифрования**.

11. Нажмите на кнопку **Импортировать ключи шифрования на Сервер администрирования**.

    Убедитесь, что пользователю, импортирующему ключи шифрования на Сервер, предоставлено право **Запись** к функции Управления ключами шифрования.

12. В окне **Импорт ключей шифрования**:

    - Нажмите на кнопку **Обзор** и выберите файл, содержащий ключи шифрования.
    - Укажите пароль.

13. Нажмите на кнопку **ОК**.

Ключи шифрования будут переданы на целевой Сервер администрирования.

Хранилища данных

Этот раздел содержит информацию о данных, которые хранятся на Сервере администрирования и используются для отслеживания состояния клиентских устройств и для их обслуживания.

Данные, которые используются для отслеживания состояния клиентских устройств и их обслуживания, отображаются в папке дерева консоли **Хранилища**.

Папка **Хранилища** содержит следующие объекты:

- загруженные Сервером администрирования обновления, которые распространяются на клиентские устройства;
- список оборудования, обнаруженного в сети;
- лицензионные ключи, обнаруженные на клиентских устройствах;
- файлы, помещенные приложениями безопасности в карантинные папки на устройствах;
- файлы, помещенные в резервные хранилища клиентских устройств;
- файлы, для которых приложения безопасности определили необходимость отложенной проверки.

Экспорт списка объектов, находящихся в хранилище, в текстовый файл

Вы можете экспортировать в текстовый файл список объектов, находящихся в хранилище.

Чтобы экспортировать в текстовый файл список объектов, находящихся в хранилище:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку нужного вам хранилища.
2. В контекстном меню списка объектов хранилища выберите пункт **Экспортировать список**.

   В результате откроется окно **Экспорт списка**, в котором вы можете указать имя текстового файла и адрес папки, в которую он будет помещен.

Инсталляционные пакеты

Kaspersky Security Center помещает в хранилища данных инсталляционные пакеты приложений "Лаборатории Касперского" и приложений сторонних производителей.

Инсталляционный пакет представляет собой набор файлов, необходимых для установки приложения. Инсталляционный пакет содержит параметры процесса установки и первоначальной конфигурации устанавливаемого приложения.

Если вы хотите установить какое-либо приложение на клиентское устройство, для этого приложения необходимо создать инсталляционный пакет или использовать уже созданный инсталляционный пакет. Список созданных инсталляционных пакетов содержится в папке дерева консоли **Удаленная установка**, во вложенной папке **Инсталляционные пакеты**.

Основные статусы файлов в хранилище

Приложения безопасности проверяют файлы на устройствах на наличие известных вирусов и других приложений, представляющих угрозу, присваивают статусы файлам и помещают некоторые файлы в хранилище.

Например, приложения безопасности могут:

- сохранять в хранилище копию файла перед удалением;
- изолировать в хранилище возможно зараженные файлы.

Основные статусы файлов приведены в таблице ниже. Вы можете получить более подробную информацию о действиях с файлами в справках приложений безопасности.

Статусы файлов в хранилище

Название статуса	Описание статуса
Заражен	В файле найден участок кода известного вируса или другой представляющей угрозу приложению, информация о котором содержится в антивирусных базах "Лаборатории Касперского".
Не заражен	В файле не обнаружено известных вирусов или других вредоносных приложений, представляющих угрозу.
Предупреждение	В файле содержится участок кода, частично совпадающий с контрольным участком кода известной угрозы.
Возможно зараженный	В файле содержится либо модифицированный код известного вируса, либо код, напоминающий вирус, пока не известный "Лаборатории Касперского".
Помещен в папку пользователем	Пользователь самостоятельно поместил файл в хранилище, например, поведение файла давало основание подозревать в нем наличие угрозы. Пользователь может проверить файл на наличие в нем угроз с помощью обновленных баз.
Ложное срабатывание	Приложение "Лаборатории Касперского" присвоило статус незараженному файлу как зараженному ввиду того, что его код напоминает код вируса. После проверки с применением обновленных баз файл определяется как незараженный.
Вылечен	Файл удалось вылечить.
Удален	Файл удален в результате обработки.
Защищен паролем	Файл не может быть обработан по причине того, что он защищен паролем.

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. 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 для Windows.

Просмотр списка обнаружений, выполненных с помощью правил Адаптивного контроля аномалий

Чтобы просмотреть список обнаружений, выполненных с помощью правил Адаптивного контроля аномалий:

1. В дереве консоли выберите требуемый узел Сервера администрирования.

2. Выберите подпапку **Правила срабатываний в статусе Интеллектуальное обучение** (по умолчанию она находится в папке **Дополнительно** → **Хранилища**).

   В списке отображается следующая информация об обнаружении, выполняемая с помощью правил Адаптивного контроля аномалий:

   - **Группа администрирования**

     Имя группы администрирования, в которую включено устройство.

   - **Имя устройства**

     Имя клиентского устройства, на котором было применено правило.

   - **Имя**

     Имя правила, которое было применено.

   - **Статус**

     Исключение – если администратор обработал это обнаружение и добавил его как исключение из правил. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

     Подтверждение – если администратор обработал это обнаружение и подтвердил его. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

     Пусто – если администратор не обработал обнаружение.

- **Количество срабатываний для всех правил**

  Количество обнаружений одного эвристического правила, одного процесса и одного клиентского устройства. Это количество рассчитано Kaspersky Endpoint Security.

- **Имя пользователя**

  Имя пользователя клиентского устройства, запустившего процесс, который сгенерировал обнаружение.

- **Путь исходного процесса**

  Путь к исходному процессу, то есть к процессу, выполнившему действие (подобную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного процесса**

  Хеш SHA256 исходного файла процесса (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь исходного объекта**

  Путь к объекту, который запустил процесс (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного объекта**

  Хеш SHA256 исходного файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого процесса**

  Путь к целевому процессу (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого процесса**

  Хеш SHA256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого объекта**

  Путь к целевому объекту (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого объекта**

  Хеш SHA256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Обработан**

  Дата обнаружения аномалии.

Чтобы просмотреть свойства каждого элемента:

1. В дереве консоли выберите требуемый узел Сервера администрирования.

2. Выберите подпапку **Правила срабатываний в статусе Интеллектуальное обучение** (по умолчанию она находится в папке **Дополнительно** → **Хранилища**).

3. В рабочей области папки **Правила срабатываний в статусе Интеллектуальное обучение** выберите нужный объект.

4. Выполните одно из следующих действий:

   - Перейдите по ссылке **Свойства** в рабочей области в правой части экрана.
   - В контекстном меню объекта выберите пункт **Свойства**.

   В открывшемся окне свойства объекта отображается информация объекта.

Вы можете подтвердить или добавить в исключения любой объект в списке, обнаруженный правилами Адаптивного контроля аномалий.

Чтобы подтвердить объект,

выберите один или несколько элементов в списке обнаружений и нажмите на кнопку **Подтвердить**.

Статус элементов будет изменен на **Подтверждение**.

Ваше подтверждение влияет на статистику, используемую правилами (подробную информацию см. в справке Kaspersky Endpoint Security 11 для Windows).

Чтобы добавить объект в исключения,

В контекстном меню объекта (или нескольких объектов) списка обнаружений выберите пункт **Добавить в исключения**.

В результате запустится мастер добавления исключений. Следуйте инструкциям мастера.

Если вы отклоните или подтвердите объект, он будет исключен из списка обнаружений после следующей синхронизации клиентского устройства с Сервером администрирования и больше не будет отображаться в списке.

Добавление исключений в правила Адаптивного контроля аномалий

Мастер добавления исключений позволяет добавлять исключения из правил Адаптивного контроля аномалий для Kaspersky Endpoint Security.

Вы можете запустить мастер с помощью одного из способов ниже.

Чтобы запустить мастер добавления исключений в папке Адаптивный контроль аномалий:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. Выберите подпапку **Правила срабатываний в статусе Интеллектуальное обучение** (по умолчанию она находится в папке **Дополнительно** → **Хранилища**).
3. В рабочей области в списке обнаружений в контекстном меню объекта (или нескольких объектов) выберите пункт **Добавить в исключения**.

   За один раз можно добавить до 1000 исключений. Если вы выберете больше элементов и попытаетесь добавить их в исключения, появится сообщение об ошибке.

В результате запустится мастер добавления исключений.

Чтобы запустить мастер добавления исключений из других узлов в дереве консоли:

- Откройте вкладку **События** главного окна Сервера администрирования, затем выберите **Запросы пользователей** или **Последние события**.
- В окне **Отчет о состоянии правил Адаптивного контроля аномалий** выберите столбец **Количество обнаружений**.

Шаг 1. Лицензирование приложения

> Этот шаг можно пропустить, если у вас есть только приложения Kaspersky Endpoint Security для Windows и нет других приложений, поддерживающих правила Адаптивного контроля аномалий.

Мастер добавления исключений отображает список приложений "Лаборатории Касперского", для которых плагины управления позволяют добавлять исключения к политикам для этих приложений. Выберите приложение из списка и нажмите на кнопку **Далее**, чтобы продолжить выбор политики, для которой будет добавлено исключение.

Шаг 2. Выбор политики (политик)

Мастер отображает список политик (с профилями политик) для Kaspersky Endpoint Security.

Выберите все политики и профили политик, в которые вы хотите добавить исключения, и нажмите на кнопку **Далее**.

Шаг 3. Обработка политики (политик)

Мастер отображает ход обработки политики. Вы можете прервать обработку политики, нажав на кнопку **Отмена**.

Унаследованные политики не могут быть обновлены. Если у вас нет прав на изменение политики, такая политика также не будет обновлена.

Когда все политики обработаны (или обработка политик прервана), создается отчет. Отчет отображает, какие политики были успешно обновлены (зеленый значок), а какие политики не были обновлены (красный значок).

Это последний шаг мастера. Нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Карантин и резервное хранилище

Приложения защиты "Лаборатории Касперского", установленные на клиентских устройствах, в процессе проверки устройств могут помещать файлы на карантин или в резервное хранилище.

Карантин – это специальное хранилище, в которое помещаются файлы, возможно зараженные вирусами или неизлечимые на момент обнаружения.

Резервное хранилище предназначено для хранения резервных копий файлов, которые были удалены или изменены в процессе лечения.

Kaspersky Security Center формирует общий список файлов, помещенных на карантин и в резервное хранилище приложениями "Лаборатории Касперского" на устройствах. Агенты администрирования клиентских устройств передают информацию о файлах на карантине и в резервных хранилищах на Сервер администрирования. Через Консоль администрирования можно просматривать свойства файлов, находящихся в хранилищах на устройствах, запускать проверку вредоносного ПО хранилищ и удалять из них файлы. Значки статусов файлов описаны в приложении.

Работа с карантином и резервным хранилищем доступна для Kaspersky Endpoint Security.

Kaspersky Security Center не копирует файлы из хранилищ на Сервер администрирования. Все файлы размещаются в хранилищах на устройствах. Восстановление файлов выполняется на устройстве, где установлено приложение безопасности, поместившее файл в хранилище.

Включение удаленного управления файлами в хранилищах

По умолчанию удаленное управление файлами в хранилищах на клиентских устройствах отключено.

Чтобы включить удаленное управление файлами в хранилищах на клиентских устройствах:

1. В дереве консоли выберите группу администрирования, для которой требуется включить удаленное управление файлами хранилищ.
2. В рабочей области группы откройте вкладку **Политики**.
3. На вкладке **Политики** выберите политику приложения безопасности, помещающей файлы в хранилища на устройствах.
4. В окне свойств политики в блоке **Информировать Сервер администрирования** установите флажки, соответствующие хранилищам, для которых вы хотите включить удаленное управление.

   Расположение блока **Информировать Сервер администрирования** в окне свойств политики и названия флажков в блоке индивидуальны для каждого приложения безопасности.

Просмотр свойств файла, помещенного в хранилище

Чтобы просмотреть свойства файла, помещенного на карантин или в резервное хранилище:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
2. В рабочей области папки **Карантин** (**Резервное хранилище**) выберите файл, параметры которого требуется просмотреть.
3. В контекстном меню файла выберите пункт **Свойства**.

Удаление файлов из хранилища

Чтобы удалить файл, помещенный на карантин или в резервное хранилище:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
2. В рабочей области папки **Карантин** (или **Резервное хранилище**) с помощью клавиш **Shift** и **Ctrl** выберите файлы, которые требуется удалить.
3. Удалите файлы одним из следующих способов:
   - В контекстном меню файлов выберите пункт **Удалить**.
   - По ссылке **Удалить** (**Удалить**) при удалении одного файла в блоке работы с выбранными файлами.

В результате приложения безопасности, поместившие выбранные файлы в хранилища на клиентских устройствах, удалят файлы из этих хранилищ.

Восстановление файлов из хранилища

Чтобы восстановить файл из карантина или резервного хранилища:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
2. В рабочей области папки **Карантин** (**Резервное хранилище**) с помощью клавиш **Shift** и **Ctrl** выберите файлы, которые требуется восстановить.
3. Запустите процесс восстановления файлов одним из следующих способов:
   - В контекстном меню файлов выберите пункт **Восстановить**.
   - По ссылке **Восстановить** в блоке работы с выбранными файлами.

В результате приложения безопасности, поместившие файлы в хранилища на клиентских устройствах, восстановят файлы в исходные папки.

Сохранение файла из хранилища на диск

Kaspersky Security Center позволяет сохранять на диск копии файлов, помещенных приложением безопасности на карантин или в резервное хранилище на клиентском устройстве. Файлы копируются на устройство, на котором установлен Kaspersky Security Center, в указанную вами папку.

Чтобы сохранить копию файла из карантина или резервного хранилища на жесткий диск:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
2. В рабочей области папки **Карантин** (**Резервное хранилище**) выберите файл, который требуется скопировать на жесткий диск.

3. Запустите процесс копирования файла одним из следующих способов:

   - В контекстном меню файла выберите пункт **Сохранить на диск**.
   - В блоке работы с выбранным файлом нажмите на ссылку **Сохранить на диск**.

В результате приложение безопасности, поместившее файл на карантин на клиентском устройстве, сохранит копию файла в указанную папку.

Сканирование файлов, находящихся на карантине

Чтобы проверить файлы, находящиеся на карантине:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин**.
2. В рабочей области папки **Карантин** с помощью клавиш **SHIFT** и **CTRL** выберите файлы, которые требуется проверить.
3. Запустите процесс проверки файлов одним из следующих способов:

   - В контекстном меню файла выберите пункт **Проверить**.
   - По ссылке **Проверить** в блоке работы с выбранными файлами.

   Приложение запускает задачу проверки по требованию для приложений безопасности, которые поместили выбранные файлы на карантин, на устройствах, где хранятся эти файлы.

Активные угрозы

Информация о необработанных файлах, обнаруженных на клиентских устройствах, содержится в папке **Хранилища**, во вложенной папке **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 дереве консоли в папке **Хранилища** выберите вложенную папку **Активные угрозы**.
2. В рабочей области папки **Активные угрозы** выберите файл, который требуется вылечить.
3. Запустите процесс лечения файла одним из следующих способов:

   - В контекстном меню файла выберите пункт **Лечить**.
   - По ссылке **Лечить** в блоке работы с выбранным файлом.

   В результате выполняется попытка лечения 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.

Сохранение необработанного файла на диск

Kaspersky Security Center позволяет сохранять на диск копии необработанных файлов, обнаруженные на клиентских устройствах. Это относится к файлам, которые обрабатываются или удаляются приложением. Файлы копируются на устройство с установленным Kaspersky Security Center в указанную папку.

Вы можете сохранить только копии файлов, которые были удалены или изменены во время лечения и их копии хранятся в хранилище Kaspersky Endpoint Security для Windows на управляемом устройстве.

Чтобы сохранить копию необработанного файла на диск:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Активные угрозы**.
2. В рабочей области папки **Активные угрозы** выберите файлы, которые требуется скопировать на диск.
3. Запустите процесс копирования файла одним из следующих способов:
   - В контекстном меню файла выберите пункт **Сохранить на диск**.
   - В блоке работы с выбранным файлом нажмите на ссылку **Сохранить на диск**.

В результате приложение безопасности клиентского устройства, на котором обнаружен выбранный необработанный файл, сохранит копию файла в указанную папку.

Удаление файлов из папки "Активные угрозы"

*Чтобы удалить файл из папки **Активные угрозы**:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Активные угрозы**.
2. В рабочей области папки **Активные угрозы** с помощью клавиш **SHIFT** и **CTRL** выберите файлы, которые требуется удалить.
3. Удалите файлы одним из следующих способов:
   - В контекстном меню файлов выберите пункт **Удалить**.
   - По ссылке **Удалить** (**Удалить**) при удалении одного файла в блоке работы с выбранными файлами.

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**.

Kaspersky Security Network (KSN)

В этом разделе описано использование инфраструктуры онлайн-служб Kaspersky Security Network (KSN). Приведена информация о KSN, а также инструкции по включению KSN, настройке доступа к KSN, по просмотру статистики использования прокси-сервера KSN.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

О KSN

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. KSN позволяет получать из репутационных баз "Лаборатории Касперского" информацию о приложениях, установленных на управляемых устройствах.

Kaspersky Security Center поддерживает следующие инфраструктурные решения:

- *KSN* – решение, позволяющее обмениваться информацией с Kaspersky Security Network. Участвуя в программе KSN, вы соглашаетесь в автоматическом режиме предоставлять в "Лабораторию Касперского" информацию о работе приложений "Лаборатории Касперского", установленных на клиентских устройствах, находящихся под управлением Kaspersky Security Center. Передача информации выполняется в соответствии с настроенными параметрами доступа к KSN. Эксперты "Лаборатории Касперского" дополнительно анализируют полученную информацию и включают ее в репутационные и статистические базы данных Kaspersky Security Network. Kaspersky Security Center использует это решение по умолчанию.

- *Kaspersky Private Security Network (KPSN)* – это решение, которое предоставляет пользователям устройств с установленными приложениями "Лаборатории Касперского" доступ к репутационным базам Kaspersky Security Network и другим статистическим данным без отправки данных со своих устройств в Глобальный KSN. KPSN предназначен для организаций, которые не могут участвовать в Kaspersky Security Network по одной из следующих причин:

  - Устройства пользователей не подключены к интернету.

  - Передача любых данных за пределы страны или корпоративной сети (LAN) запрещена законом или корпоративными политиками безопасности.

  Вы можете настроить параметры доступа Kaspersky Private Security Network в разделе **Параметры прокси-сервера KSN** окна свойств Сервера администрирования.

Приложение предлагает присоединиться к KSN во время работы мастера первоначальной настройки. Вы можете начать использование KSN или отказаться от использования KSN в любой момент работы с приложением.

Вы используете KSN в соответствии с Положением о KSN, которое вы читаете и принимаете при включении KSN. Если Положение о KSN обновлено, оно отображается при обновлении Сервера администрирования с предыдущей версии. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с предыдущей версией Положения о KSN, которую вы приняли ранее.

Когда KSN включен, Kaspersky Security Center 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, получать информацию от KSN и передавать в KSN информацию, даже если они не имеют прямого доступа в интернет.
- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентским устройством запрошенной информации.

Вы можете настроить параметры прокси-сервера KSN в разделе **Параметры прокси-сервера KSN** окна свойств Сервера администрирования.

Настройка доступа к Kaspersky Security Network

Можно задать доступ к Kaspersky Security Network (KSN) с Сервера администрирования и с точки распространения.

Чтобы настроить доступ Сервера администрирования к Kaspersky Security Network (KSN):

1. В дереве консоли выберите Сервер администрирования, для которого нужно настроить доступ к KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Прокси-сервер KSN** → **Параметры прокси-сервера KSN**.
4. Установите флажок **Использовать Сервер администрирования как прокси-сервер**, чтобы использовать службу прокси-сервера KSN.

   Передача данных от клиентских устройств в KSN регулируется политикой Kaspersky Endpoint Security, действующей на клиентских устройствах. Если флажок снят, передача данных в KSN от Сервера администрирования и от клиентских устройств через Kaspersky Security Center не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky Security Center). Действующая на клиентских устройствах политика Kaspersky Endpoint Security для Windows определяет, какие данные эти устройства напрямую (не через Kaspersky Security Center) передают в KSN.
5. Включите параметр **Я принимаю условия использования Kaspersky Security Network**.

   Если параметр включен, клиентские устройства будут передавать результаты установки патчей в "Лабораторию Касперского". При включении этого параметра убедитесь, что вы прочитали и принимаете условия Положения о KSN.

Если вы используете Kaspersky Private Security Network, включите параметр **Настроить KPSN** и нажмите на кнопку **Файл с параметрами прокси-сервера KSN**, чтобы загрузить параметры KPSN (файлы с расширениями pkcs7 и pem). После загрузки параметров в интерфейсе отображаются наименование провайдера, контакты провайдера и дата создания файла с параметрами KPSN.

При включении KPSN обратите внимание на точки распространения настроенные на отправление KSN запросов напрямую облачной-службе KSN. Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к облачной-службе KSN. Чтобы перенастроить точки распространения для отправки запросов KSN в KPSN, включите параметр **Пересылать KSN запрос Серверу администрирования** для каждой точки распространения. Вы можете включить этот параметр в свойствах точки распространения или политики Агента администрирования.

Когда вы устанавливаете флажок **Настроить KPSN**, появляется сообщение с информацией о KPSN.

Если вы включите параметр **Настроить KPSN** в Kaspersky Security Center, эти приложения получат об этом информацию о поддержке KPSN. В окне свойств приложения в подразделе **Kaspersky Security Network** раздела **Продвинутая защита** отображается поставщик KSN: KSN или KPSN.

Если для работы с KPSN вы используете версии приложений ниже Kaspersky Security для виртуальных сред 3.0 Защита без агента Service Pack 2 или ниже Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент, рекомендуется использовать подчиненные Серверы администрирования, для которых не настроено использование KPSN.

Kaspersky Security Center не отправляет статистику Kaspersky Security Network, если настроен KPSN в окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** → **Параметры прокси-сервера KSN**.

Установите флажок **Игнорировать параметры прокси-сервера для подключения к KPSN**, если в свойствах Сервера администрирования настроены параметры прокси-сервера, но архитектура сети требует работы с KPSN напрямую. В противном случае запрос от управляемого приложения не будет передан в KPSN.

6. Настройте параметры подключения Сервера администрирования к службе прокси-сервера KSN:

   - В блоке **Параметры подключения**, в поле ввода **TCP-порт**, укажите номер TCP-порта, через который будет выполняться подключение к прокси-серверу KSN. По умолчанию подключение к прокси-серверу KSN выполняется через порт 13111.

   - Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, выберите параметр **Использовать UDP-порт** и в поле **UDP-порт** укажите номер порта. По умолчанию параметр выключен, используется порт TCP. Если параметр включен, по умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

   - Чтобы Сервер администрирования подключался к прокси-серверу KSN через HTTPS-порт, включите параметр **Использовать HTTPS через порт** и укажите номер порта. По умолчанию параметр выключен, используется порт TCP. Если параметр включен, по умолчанию подключение к прокси-серверу KSN выполняется через HTTPS-порт 17111.

7. Включите параметр **Подключать подчиненные Серверы администрирования к KSN через главный Сервер**.

Если этот параметр включен, подчиненные Серверы администрирования на любом уровне иерархии используют главный Сервер администрирования в качестве прокси-сервера KSN. Если этот параметр выключен, подчиненные Серверы администрирования подключаются к KSN самостоятельно. В этом случае управляемые устройства используют подчиненные Серверы администрирования как прокси-серверы KSN.

Подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера, если в свойствах подчиненных Серверов администрирования в разделе **Параметры прокси-сервера KSN** также установлен флажок **Использовать Сервер администрирования как прокси-сервер**.

8. Нажмите на кнопку **OK**.

В результате параметры доступа к KSN будут сохранены.

Можно также настроить доступ к KSN со стороны точки распространения, например, если необходимо снизить нагрузку на Сервер администрирования. Точка распространения, выполняющая роль прокси-сервера KSN, отправляет KSN запросы от управляемых устройств напрямую в "Лабораторию Касперского", минуя Сервер администрирования.

Чтобы настроить доступ точки распространения к Kaspersky Security Network (KSN):

1. Убедитесь, что точка распространения была назначена вручную.
2. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
3. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
4. В окне свойств Сервера администрирования выберите раздел **Точки распространения**.
5. Выберите в списке точку распространения и по кнопке **Свойства** откройте окно ее свойств.
6. В окне свойств точки распространения в разделе **Прокси-сервер KSN** выберите **Доступ к облачной службе KSN/KPSN непосредственно через интернет**.
7. Нажмите на кнопку **OK**.

Точка распространения будет исполнять роль прокси-сервера KSN.

Включение и отключение KSN

Чтобы включить KSN:

1. В дереве консоли выберите Сервер администрирования, для которого нужно включить KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите подраздел **Параметры прокси-сервера KSN**.
4. Выберите **Использовать Сервер администрирования как прокси-сервер**.

   В результате будет включена служба прокси-сервера KSN.

5. Установите флажок **Я принимаю условия использования Kaspersky Security Network**.

   В результате KSN будет включен.

   Если флажок установлен, клиентские устройства будут передавать результаты установки патчей в "Лабораторию Касперского". Установив флажок, вам нужно прочитать и принять условия Положения о KSN.

6. Нажмите на кнопку **OK**.

Чтобы выключить KSN:

1. В дереве консоли выберите Сервер администрирования, для которого нужно включить KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите подраздел **Параметры прокси-сервера KSN**.
4. Снимите флажок **Использовать Сервер администрирования как прокси-сервер**, чтобы выключить службу прокси-сервера KSN, или снимите флажок **Я принимаю условия использования Kaspersky Security Network**.

   Если флажок снят, клиентские устройства не будут передавать результаты установки патчей в "Лабораторию Касперского".

   Если вы используете KPSN, снимите флажок **Настроить KPSN**.

   В результате KSN будет выключен.

5. Нажмите на кнопку **OK**.

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 дереве консоли выберите Сервер администрирования, для которого включен KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите подраздел **Параметры прокси-сервера KSN**.
4. Перейдите по ссылке **Просмотреть принятые Положения о KSN**.

В открывшемся окне вы можете просмотреть текст принятого Положения о KSN.

Просмотр статистики прокси-сервера KSN

Прокси-сервер KSN – это служба, обеспечивающая взаимодействие между инфраструктурой Kaspersky Security Network и клиентскими устройствами, находящимися под управлением Сервера администрирования.

Использование прокси-сервера KSN предоставляет вам 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.

В окне свойств Сервера администрирования вы можете настроить параметры прокси-сервера KSN и просмотреть статистическую информацию об использовании прокси-сервера KSN.

Чтобы просмотреть статистику работы прокси-сервера KSN:

1. В дереве консоли выберите Сервер администрирования, для которого нужно просмотреть статистику KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите подраздел **Статистика прокси-сервера KSN**.

   В этом разделе отображается фактическая статистика работы прокси-сервера KSN (количество записей в кеше, количество обработанных пакетов в кеше и полученных пакетов). Также, если Сервер администрирования подключен к KSN, отображается соответствующее информационное сообщение.

   Если необходимо, выполните дополнительные действия:

   - по кнопке **Обновить** обновите статистическую информацию об использовании прокси-сервера KSN;
   - по кнопке **Экспортировать в файл** экспортируйте данные статистики в файл формата CSV;
   - по кнопке **Проверить подключение к KSN** проверьте, подключен ли Сервер администрирования к KSN в настоящий момент.
4. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств Сервера администрирования.

Принятие обновленного Положения о KSN

Вы используете KSN в соответствии с Положением о KSN, которое вы читаете и принимаете при включении KSN. Если Положение о KSN обновлено, оно отображается при обновлении Сервера администрирования или при обновлении Сервера администрирования с предыдущей версии. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с версией Положения о KSN, которую вы приняли ранее.

После обновления Сервера администрирования или после обновления с предыдущей версии Сервера администрирования, обновленное Положение о KSN отображается автоматически. Если вы отклоните обновленное Положение о KSN, вы все равно сможете просмотреть и принять его позже.

Чтобы просмотреть и принять или отклонить обновленное Положение о KSN:

1. В дереве консоли выберите узел **Сервер администрирования**.

2. На вкладке **Мониторинг** в разделе **Мониторинг** перейдите по ссылке **Принятое Положение о Kaspersky Security Network устарело**.

   Откроется окно **Положение о KSN**.

3. Внимательно прочтите Положение о KSN, а затем примите решение. Если вы принимаете условия обновленного Положения о KSN, нажмите на кнопку **Я принимаю условия Лицензионного соглашения**. Если вы отклоняете условия обновленного Положения о KSN, нажмите на кнопку **Отмена**.

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.

Дополнительная защита с использованием Kaspersky Security Network

«Лаборатория Касперского» предоставляет дополнительный уровень защиты с использованием Kaspersky Security Network. Этот способ защиты нацелен на эффективную борьбу против постоянных угроз повышенной сложности и угроз нулевого дня. Объединенные с Kaspersky Endpoint Security облачные технологии и экспертные знания вирусных аналитиков «Лаборатории Касперского» обеспечивают мощную защиту против сложнейших угроз в сети.

Более подробную информацию о дополнительной защите в Kaspersky Endpoint Security вы можете найти на веб-сайте «Лаборатории Касперского».

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.

Переключение между онлайн-справкой и офлайн-справкой

Если у вас нет доступа в интернет, вы можете использовать офлайн-справку.

Чтобы переключиться между онлайн-справкой и офлайн-справкой:

1. В главном окне Kaspersky Security Center в дереве консоли выберите узел **Kaspersky Security Center 15.1**.

2. Перейдите по ссылке **Параметры общего интерфейса**.

   Откроется окно параметров.

3. В окне свойств нажмите на ссылку **Использовать офлайн-справку**.

4. Нажмите на кнопку **OK**.

   Параметры применены и сохранены. Вы можете в любой момент изменить параметры и начать пользоваться онлайн-справкой в любое время.

Export of events to SIEM systems

This section explains how to export events registered by Kaspersky Security Center to external Security Information and Event Management (SIEM) systems.

Настройка экспорта событий в SIEM-системы

Kaspersky Security Center позволяет выполнять настройку одним из способов: экспорт в любую SIEM-систему, использующую формат Syslog, экспорт в QRadar, Splunk, ArcSight SIEM-системы, использующие форматы LEEF и CEF, или экспорт событий в SIEM-системы прямо из базы Kaspersky Security Center. По завершении этого сценария Сервер администрирования автоматически отправляет события в SIEM-систему.

Предварительные требования

Перед началом настройки экспорта событий в Kaspersky Security Center:

- Узнайте больше о методах экспорта событий.
- Убедитесь, что у вас есть значения системных параметров.

Вы можете выполнять шаги этого сценария в любом порядке.

Процесс экспорта событий в SIEM-систему состоит из следующих шагов:

- **Настройка SIEM-системы для получения событий из Kaspersky Security Center**

  Инструкции: Настройка экспорта событий в SIEM-системе.

- **Выбор события, которые вы хотите экспортировать в SIEM-систему:**

  Инструкции:

  - Консоль администрирования: Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog, Выбор общих событий для экспорта в формате Syslog.
  - Kaspersky Security Center Web Console: Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog, Выбор общих событий для экспорта в формате Syslog.

- **Настройка экспорта событий в SIEM-систему одним из следующих способов:**

  - Использование протоколов TCP, UDP или TLS over TCP.

    Инструкции:

    - Консоль администрирования: Настройка экспорта событий в SIEM-системы.
    - Kaspersky Security Center Web Console: Настройка экспорта событий в SIEM-системы.

  - Использование экспорта событий напрямую из базы данных Kaspersky Security Center. В базе данных Kaspersky Security Center представлен набор публичных представлений; вы можете найти описание этих общедоступных представлений в документе klakdb.chm.

Результаты

После настройки экспорта событий в SIEM-систему вы можете просматривать результаты экспорта, если вы выбрали события, которые хотите экспортировать.

Предварительные условия

При настройке автоматического экспорта событий в Kaspersky Security Center необходимо указать некоторые параметры SIEM-системы. Рекомендуется уточнить эти параметры заранее, чтобы подготовиться к настройке Kaspersky Security Center.

Для настройки автоматического экспорта событий в SIEM-систему необходимо знать значения следующих параметров:

- **Адрес сервера SIEM-системы**

  Адрес сервера, на котором установлена используемая SIEM-система. Это значение необходимо уточнить в настройках SIEM-системы.

- **Порт сервера SIEM-системы**

  Номер порта, по которому будет установлено соединение между Kaspersky Security Center и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

- **Протокол**

  Протокол, используемый для передачи сообщений из Kaspersky Security Center в SIEM-систему. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

О событиях в Kaspersky Security Center

Kaspersky Security Center позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования. 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 администрирования.

Типы событий

В Kaspersky Security Center существуют следующие типы уведомлений:

- Общие события. Эти события возникают во всех управляемых приложениях "Лаборатории Касперского". Например, общее событие Вирусная атака. Общие события имеют строго определенные синтаксис и семантику. Общие события используются, например, в отчетах и панели мониторинга.

- Специфические события управляемых приложений "Лаборатории Касперского". Каждое управляемое приложение "Лаборатории Касперского" имеет собственный набор событий.

Источники событий

События могут генерироваться следующими приложениями:

- Компоненты приложения Kaspersky Security Center:
  - Сервер администрирования
  - Агент администрирования
  - Сервер iOS MDM
- Управляемые приложения "Лаборатории Касперского"

  Подробнее о событиях, генерируемых управляемыми приложениями "Лаборатории Касперского", см. в документации соответствующего приложения.

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.

Уровень важности события

Каждое событие имеет собственный уровень важности. В зависимости от условий возникновения, событию могут быть присвоены различные уровни важности. Существует четыре уровня важности событий:

- *Критическое событие* – событие, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.
- *Отказ функционирования* – событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы приложения или выполнения процедуры.
- *Предупреждение* – событие, не обязательно являющееся серьезным, однако указывающее на возможное возникновение проблемы в будущем. Чаще всего события относятся к Предупреждениям, если после их возникновения работа приложения может быть восстановлена без потери данных или функциональных возможностей.
- *Информационное сообщение* – событие, возникающее с целью информирования об успешном выполнении операции, корректной работе приложения или завершении процедуры.

Для каждого события задано время хранения, которое можно посмотреть или изменить в Kaspersky Security Center. Некоторые события не сохраняются в базе данных Сервера администрирования по умолчанию, поскольку для них установленное время хранения равно нулю. Во внешние системы можно экспортировать только те события, которые хранятся в базе данных Сервера администрирования не менее одного дня.

Об экспорте событий

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 во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center и получатель событий – SIEM-система. Для успешного экспорта событий необходимо выполнить настройки и в используемой SIEM-системе, и в Kaspersky Security Center. Последовательность настройки не имеет значения: Вы можете либо сначала настроить отправку событий в Kaspersky Security Center, а затем получение событий в SIEM-системе, либо наоборот.

Способы отправки событий из Kaspersky Security Center

Существует три способа отправки событий из Kaspersky Security Center во внешние системы:

- Отправка событий по протоколу Syslog в любую SIEM-систему.

  По протоколу syslog можно передавать любые события, произошедшие на Сервере администрирования Kaspersky Security Center и в приложениях "Лаборатории Касперского", установленных на управляемых устройствах. Протокол Syslog – это стандартный протокол регистрации сообщений. Вы можете использовать этот протокол для экспорта событий в любую SIEM-систему.

  Для этого нужно отметить события, которые вы хотите передать в SIEM-систему. Вы можете отметить события с помощью Консоли администрирования или Kaspersky Security Center Web Console). Только отмеченные события будут передаваться в SIEM-систему. Если вы ничего не отметили, никакие события не будут передаваться.

- Отправка событий по протоколам CEF и LEEF в системы QRadar, Splunk и ArcSight.

  Протоколы CEF и LEEF можно использовать для экспорта общих событий. При экспорте событий по протоколам CEF и LEEF у вас нет возможности выбора определенных экспортируемых событий. Вместо этого выполняется экспорт всех общих событий. Для конвертации событий Kaspersky Security Center в события формата CEF и LEEF используется файл siem_conversion_rules.xml. Этот файл содержит список атрибутов событий Kaspersky Security Center и соответствующие атрибуты событий в формате CEF и LEEF. Также файл siem_conversion_rules.xml содержит правила генерации сообщений, соответствующих событиям. Файл входит в состав комплекта поставки Kaspersky Security Center.

  В отличие от протокола syslog, протоколы CEF и LEEF не являются универсальными. Протоколы CEF и LEEF предназначены для соответствующих SIEM-систем (QRadar, Splunk и ArcSight). Поэтому при выборе экспорта событий по одному из этих протоколов в SIEM-системе используется нужный анализатор.

- Напрямую из базы данных Kaspersky Security Center в любую SIEM-систему.

  Этот способ экспорта событий можно использовать для получения событий напрямую из публичных представлений базы данных с помощью SQL-запросов. Результаты выполнения запроса сохраняются в файл XML, который можно использовать в качестве входных данных для внешней системы. Напрямую из базы данных можно экспортировать только события, доступные в публичных представлениях.

Получение событий SIEM-системой

SIEM-система должна принимать и корректно анализировать события, получаемые из Kaspersky Security Center. Для этого необходимо правильно настроить SIEM-систему. Конфигурация зависит от конкретной используемой SIEM-системы. Однако в конфигурациях всех SIEM-систем существует ряд общих этапов, таких как настройка приемника и анализатора.

О настройке экспорта событий в SIEM-системе

В процедуре экспорта событий из Kaspersky Security Center во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center и получатель событий – SIEM-система. Экспорт событий необходимо настроить в используемой SIEM-системе и в Kaspersky Security Center.

Настройки, выполняемые в SIEM-системе, зависят от того, какую систему вы используете. В общем случае для всех SIEM-систем необходимо настроить приемник сообщений и, при необходимости, анализатор сообщений, для того чтобы разложить полученные сообщения на поля.

Настройка приемника сообщений

Для SIEM-системы необходимо настроить приемник для получения событий, отправляемых Kaspersky Security Center. В общем случае в SIEM-системе необходимо указать следующие параметры:

- **Протокол экспорта или тип входных данных**

  Это протокол передачи сообщений, например UDP. Необходимо указать тот же протокол, который был выбран в Kaspersky Security Center для передачи событий.

- **Порт**

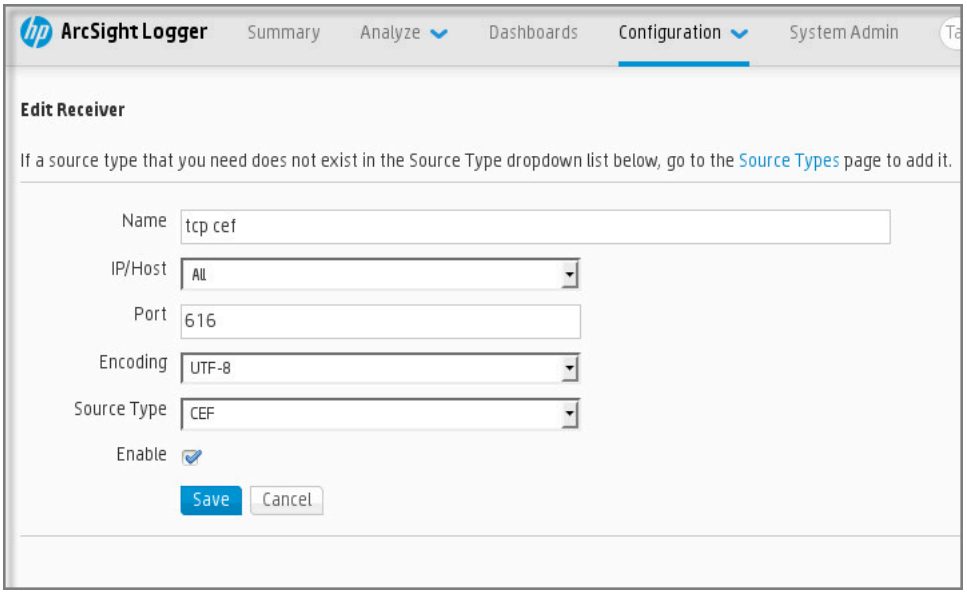
  Номер порта для подключения к Kaspersky Security Center. Необходимо указать тот же номер порта, который был выбран в Kaspersky Security Center для передачи событий.

- **Протокол передачи сообщений или тип исходных данных**

  Протокол, используемый для экспорта событий в SIEM-систему. Это может являться одним из стандартных протоколов: Syslog, CEF или LEEF. SIEM-система выбирает анализатор событий, соответствующий указанному протоколу.

В зависимости от используемой SIEM-системы может потребоваться указать дополнительные параметры приемника сообщений.

На рисунке ниже приведен пример настройки приемника в ArcSight.



Настройка приемника в ArcSight

Анализатор сообщений

Экспортируемые события передаются в SIEM-систему в виде сообщений. Затем к этим сообщениям применяется анализатор, чтобы информация о событиях могла быть использована SIEM-системой. Анализатор сообщений встроен в SIEM-систему; он используется для разбиения содержимого сообщения на соответствующие поля, такие как код события, уровень важности, описание, параметры. В результате SIEM-система имеет возможность выполнять обработку событий, полученных из Kaspersky Security Center, 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 отдельном управляемом приложении, установленном на управляемом устройстве, выберите для приложения события для экспорта. В случае, если ранее экспортируемые события были выбраны в политике, вам не удастся переопределить выбранные события для отдельного приложения, управляемой этой политикой.

Чтобы выбрать события для отдельного управляемого приложения:

1. В дереве консоли Kaspersky Security Center выберите узел **Управляемые устройства** и перейдите на вкладку **Устройства**.

2. Откройте контекстное меню требуемого устройства по правой клавише мыши и выберите пункт **Свойства**.

3. В открывшемся окне свойств устройства выберите раздел **Приложения**.

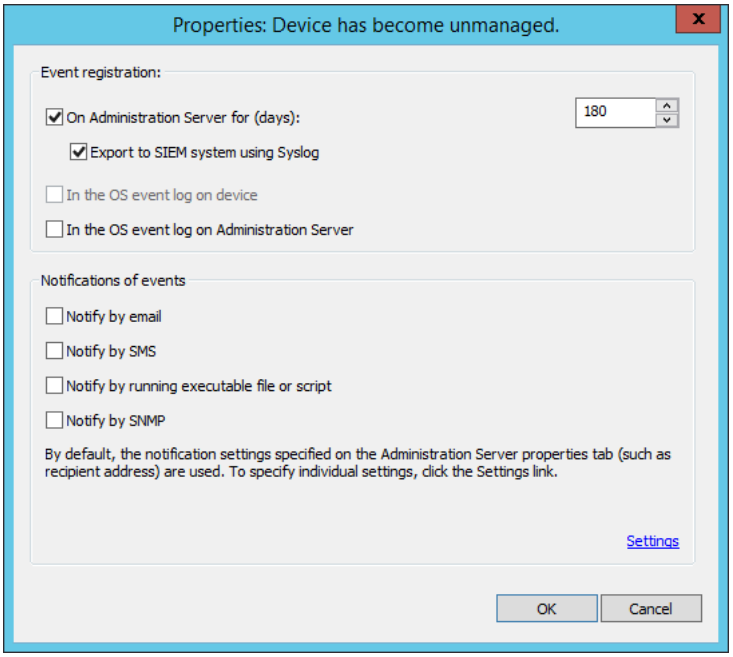
4. В появившемся списке приложений выберите приложение, события которой требуется экспортировать, и нажмите на кнопку **Свойства**.

5. В окне свойств приложения выберите раздел **Настройка событий**.

6. В появившемся списке событий выберите одно или несколько событий, которые требуется экспортировать в SIEM-систему, и нажмите на кнопку **Свойства**.

7. В открывшемся окне свойств событий выберите параметр **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы отметить выбранные события для экспорта в формате Syslog. Выключите параметр **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы отменить выбор событий для экспорта в формате Syslog.

Если свойства события заданы в политике, поля этого окна недоступны для редактирования.



Окно свойств событий

8. Нажмите на кнопку **OK**, чтобы сохранить изменения.

9. Нажмите на кнопку **OK** в окне свойств приложения и в окне свойств устройства.

Выбранные события будут отправляться в SIEM-систему в формате Syslog. События, выбор которых вы отменили параметром **Экспортировать в SIEM-систему по протоколу Syslog**, не будут экспортироваться в SIEM-систему. Экспорт начнется сразу после того, как вы включите автоматический экспорт и выберете экспортируемые события. Выполните настройку SIEM-системы, чтобы обеспечить получение событий из Kaspersky Security Center.

Выбор общих событий для экспорта в формате Syslog

Если вы хотите выполнить экспорт событий, произошедших во всех приложениях, управляемых определенной политикой, выберите экспортируемые события в политике. В этом случае вы не можете выбрать события для отдельного управляемого приложения.

Чтобы выбрать общие события для экспорта в SIEM-систему:

1. В дереве консоли Kaspersky Security Center выберите узел **Политики**.

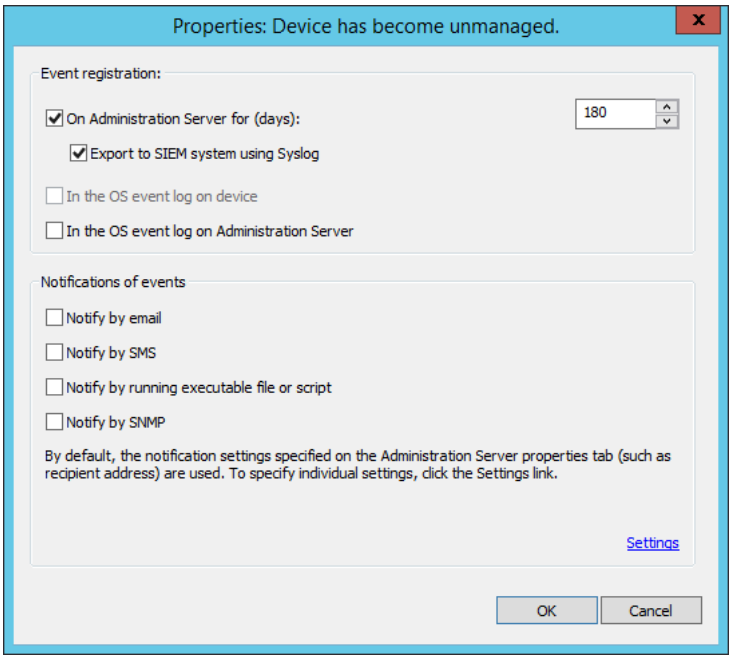
2. Откройте контекстное меню требуемой политики по правой клавише мыши и выберите пункт **Свойства**.

3. В открывшемся окне свойств политики выберите раздел **Настройка событий**.

4. В появившемся списке событий выберите одно или несколько событий, которые требуется экспортировать в SIEM-систему, и нажмите на кнопку **Свойства**.

   Если требуется выбрать все события, нажмите на кнопку **Выделить все**.

5. В открывшемся окне свойств событий выберите параметр **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы отметить выбранные события для экспорта в формате Syslog. Снимите флажок **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы отменить выбор событий для экспорта в формате Syslog.



Окно свойств событий Сервера администрирования

6. Нажмите на кнопку **OK**, чтобы сохранить изменения.

7. В окне свойств политики нажмите на кнопку **OK**.

Выбранные события будут отправляться в SIEM-систему в формате Syslog. События, выбор которых вы отменили параметром **Экспортировать в SIEM-систему по протоколу Syslog**, не будут экспортироваться в SIEM-систему. Экспорт начнется сразу после того, как вы включите автоматический экспорт и выберете экспортируемые события. Выполните настройку SIEM-системы, чтобы обеспечить получение событий из Kaspersky Security Center.

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 во внешние системы.

В Kaspersky Security Center можно настроить экспорт событий во внешние системы в формате Syslog.

Процесс экспорта состоит из двух шагов:

1. Включение автоматического экспорта событий. На этом шаге выполняется настройка Kaspersky Security Center таким образом, чтобы выполнялась отправка событий в SIEM-систему. Отправка событий из Kaspersky Security Center начинается сразу после включения автоматического экспорта.

2. Выбор событий, которые будут экспортироваться во внешнюю систему. На этом шаге вам нужно выбрать, какие события будут экспортироваться в SIEM-систему.

Об экспорте событий в форматах CEF и LEEF

Форматы CEF и LEEF можно использовать для экспорта в SIEM-систему общих событий, а также событий, переданных приложениями "Лаборатории Касперского" Серверу администрирования. Набор экспортируемых событий определен заранее, возможность выбирать экспортируемые события отсутствует. Перед отправкой событий в SIEM-систему (QRadar, ArcSight или Splunk) необходимо интерпретировать события Kaspersky Security Center в события в формате CEF и LEEF, используя правила, указанные в файле siem_conversion_rules.xml.

Формат экспорта можно выбрать в зависимости от того, какую SIEM-систему вы используете. В следующей таблице приведены SIEM-системы и соответствующие им форматы экспорта.

Форматы экспорта событий в SIEM-систему

SIEM-система	Формат экспорта
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) – это специализированный формат событий для IBM Security QRadar SIEM. QRadar может получать, идентифицировать и обрабатывать события, передаваемые по протоколу LEEF. Для протокола LEEF должна использоваться кодировка UTF-8. Более подробную информацию о протоколе LEEF см. на веб-странице IBM Knowledge Center.

- CEF – это стандарт управления типа "открытый журнал", который улучшает совместимость информации системы безопасности от разных сетевых устройств и приложений. Протокол CEF позволяет использовать общий формат журнала событий, чтобы системы управления предприятием могли легко получать и объединять данные для анализа. Для протокола CEF должна использоваться кодировка UTF-8.

При автоматическом экспорте Kaspersky Security Center отправляет общие события в SIEM-систему. Автоматический экспорт событий начинается сразу после включения. В этом разделе описана процедура включения автоматического экспорта событий.

Настройка Kaspersky Security Center для экспорта событий в SIEM-систему

Вы можете включить автоматический экспорт событий в Kaspersky Security Center.

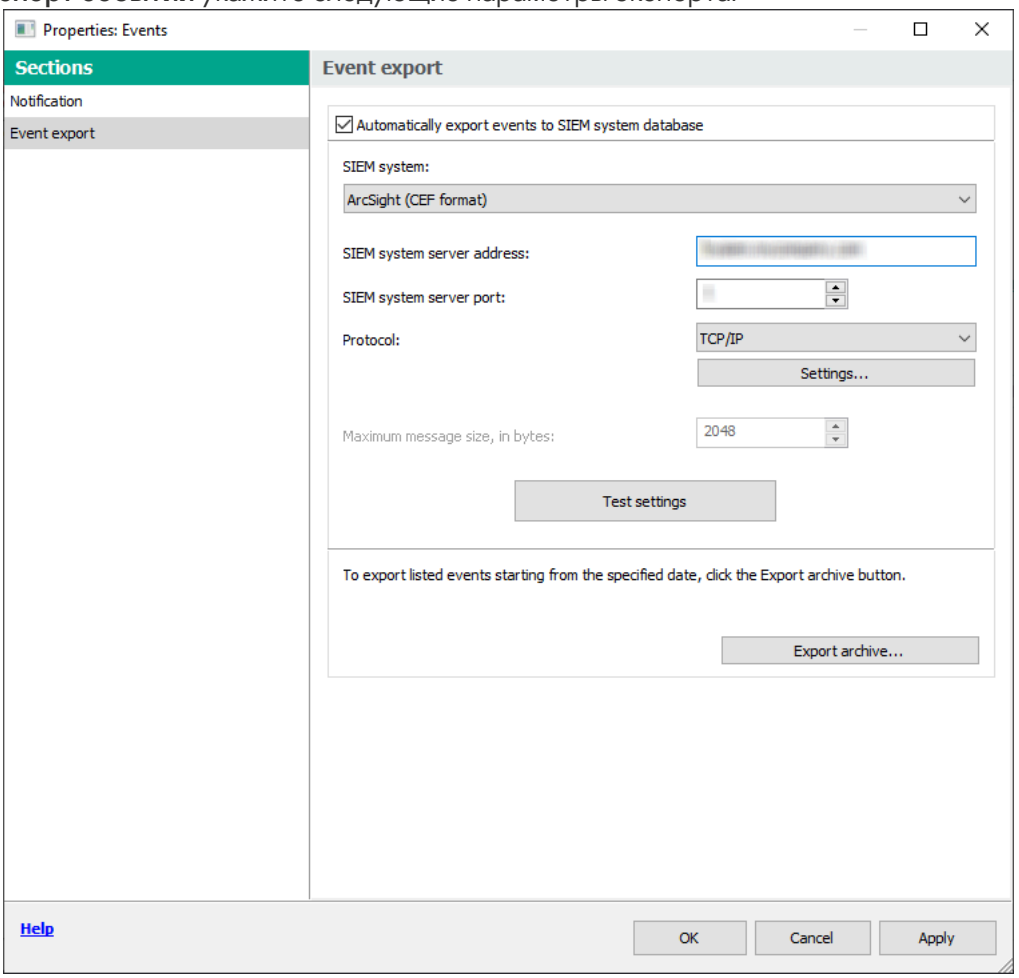
Только общие события могут быть экспортированы от управляемых приложений в форматах CEF и LEEF. Правила интерпретации, используемые для конвертации событий в форматы CEF и LEEF, задаются в файле siem_conversion_rules.xml, который входит в комплект поставки Kaspersky Security Center. Специфические события приложений не могут быть экспортированы от управляемых приложений в форматах CEF и LEEF. Если необходимо экспортировать события управляемых приложений или пользовательский набор событий, который настроен с помощью политик управляемых приложений, используйте экспорт событий в формате Syslog.

Чтобы включить автоматический экспорт общих событий:

1. В дереве консоли Kaspersky Security Center выберите узел с именем Сервера администрирования, события которого необходимо экспортировать.
2. В рабочей области выбранного Сервера администрирования перейдите на вкладку **События**.
3. Нажмите на стрелку рядом со ссылкой **Настроить параметры уведомлений и экспорта событий** и в раскрывающемся списке выберите пункт **Настроить экспорт в SIEM-систему**.

   Откроется окно свойств событий на разделе **Экспорт событий**.

4. В разделе **Экспорт событий** укажите следующие параметры экспорта:



Раздел Экспорт событий окна свойств событий

- **Автоматически экспортировать события в базу SIEM-системы**

  Установите этот флажок, для того чтобы включить автоматический экспорт событий в SIEM-систему. При установке этого флажка все поля в разделе **Экспорт событий** становятся доступными для редактирования.

- **SIEM-система**

  Выберите, в какую SIEM-систему будет выполняться экспорт событий: QRadar® (LEEF-формат), ArcSight (CEF-формат), Splunk® (CEF-формат) и формат Syslog (RFC 5424).

  Если вы выбрали формат Syslog, вам нужно указать:

  Максимальный размер сообщения в байтах

  Укажите максимальный размер в байтах одного сообщения, передаваемого в SIEM-систему. Каждое событие передается одним сообщением. Если реальная длина сообщения превышает указанное значение, сообщение обрезается и данные могут быть утеряны. По умолчанию размер сообщения составляет 2048 байт. Данное поле доступно только в случае, если вы выбрали формат Syslog в поле **SIEM-система**.

- **Адрес сервера SIEM-системы**

  Укажите адрес сервера SIEM-системы. Адрес сервера можно указать в формате DNS- или NetBIOS-имени или IP-адреса.

- **Порт сервера SIEM-системы**

  Укажите номер порта для соединения с сервером SIEM-системы. Этот номер порта должен совпадать с номером порта, который вы указываете в настройках приемника SIEM-системы для получения событий (см. раздел Настройка SIEM-системы).

- **Протокол**

  Выберите протокол передачи сообщений в SIEM-систему. Вы можете выбрать протокол TCP, UDP или TLS over TCP.

  Укажите следующие параметры TLS, если вы выбираете TLS over TCP:

  - **Аутентификация на SIEM-сервере**

    Выберите один из следующих способов аутентификации сервера SIEM-системы:

    - **Использовать сертификаты ЦС**. Вы можете получить файл со списком сертификатов от доверенного центра сертификации (CA) и загрузить его в Kaspersky Security Center. Kaspersky Security Center проверяет, подписан ли сертификат SIEM-системы также доверенным центром сертификации или нет.

      Чтобы добавить доверенный сертификат, нажмите на кнопку **Обзор** и загрузите сертификат.

      Если вы выберете параметр **Использовать сертификаты ЦС**, можно указать имена субъектов в поле **Субъекты сертификатов сервера (необязательно)**. *Имя субъекта* – это доменное имя, для которого получен сертификат. Kaspersky Security Center 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 субъекта изменилось в сертификате. Для этого укажите имена субъектов в поле **Субъекты сертификатов сервера (необязательно)**. Если какое-либо из указанных имен субъектов совпадает с именем субъекта сертификата SIEM-системы, Kaspersky Security Center проверяет сертификат сервера SIEM-системы.

    - **Используя SHA1 отпечатки сертификатов сервера**. Вы можете указать в Kaspersky Security Center SHA-1 отпечатки сертификатов SIEM-системы. Чтобы добавить отпечаток SHA-1, введите его в поле под параметром.

  - **Проверка подлинности клиента**

Для аутентификации клиента вы можете вставить свой сертификат или сгенерировать его в Kaspersky Security Center.

- **Вставить сертификат**. Вы можете использовать сертификат, полученный из любого источника, например, от любого доверенного центра сертификации. Чтобы вставить существующий сертификат нажмите на кнопку **Поиск сертификата**. В открывшемся окне **Сертификат** выберите один из следующих типов сертификатов, а затем укажите сертификат и его закрытый ключ:

  - **X.509-сертификат**. Загрузите файл с закрытым ключом в поле **Закрытый ключ (*.prk, *.pem)** и файл с сертификатом в поле **Сертификат (*.cer)**. Для этого нажмите на кнопку **Обзор** справа от соответствующего поля, а затем добавьте нужный файл. Оба файла не зависят друг от друга. Порядок загрузки файлов не имеет значения. Когда оба файла будут загружены, укажите пароль для расшифровки закрытого ключа в поле **Пароль**. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

  - **Контейнер PKCS#12**. Загрузите один файл, содержащий сертификат и его закрытый ключ, в поле **Файл сертификата**. Для этого нажмите на кнопку **Обзор** справа от поля и добавьте нужный файл. Когда файл будет загружен, укажите пароль для расшифровки закрытого ключа в поле **Пароль**. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

- **Сгенерировать ключ**. Вы можете сгенерировать самоподписанный сертификат в Kaspersky Security Center. Нажмите на кнопку **Сформировать сертификат** и введите имя субъекта в поле **Субъект**. Пользовательский сертификат создается для этого имени субъекта и отпечаток SHA-1 этого сертификата отображается в поле **Отпечаток SHA1 пользовательского сертификата**. В результате Kaspersky Security Center сохраняет сгенерированный самоподписанный сертификат, и вы можете передать публичную часть сертификата или отпечаток SHA-1 в SIEM-систему.

5. Если требуется выполнить экспорт в SIEM-систему событий, произошедших после определенной даты в прошлом, нажмите на кнопку **Экспортировать архив** и укажите дату, начиная с которой будет выполнен экспорт событий. По умолчанию экспорт событий начинается сразу после включения.

6. Чтобы убедиться, что соединение с SIEM-системой настроено, нажмите на кнопку **Проверить соединение**.

   Приложение пытается установить соединение с сервером SIEM-системы и отправить тестовое событие. Если подключение не установлено, отобразится сообщение об ошибке. Если подключение установлено, никакое сообщение не отображается. При необходимости вы можете просмотреть тестовое событие на вкладке **События**.

7. Нажмите на кнопку **ОК**.

Автоматический экспорт событий включен.

После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться в SIEM-систему.

Экспорт событий напрямую из базы данных

Вы можете извлекать события напрямую из базы данных Kaspersky Security Center, не используя интерфейс Kaspersky Security Center. Можно создавать запросы непосредственно к публичным представлениям и извлекать из них данные о событиях или создавать собственные представления на базе существующих публичных представлений и обращаться к ним для получения требуемых данных.

Публичные представления

Для вашего удобства в базе данных Kaspersky Security Center предусмотрен набор публичных представлений. Описание публичных представлений приведено в документе klakdb.chm.

Публичное представление v_akpub_ev_event содержит набор полей, соответствующих параметрам событий в базе данных. В документе klakdb.chm также содержится информация о публичных представлениях, относящихся к другим объектам Kaspersky Security Center, например, устройствам, приложениям, пользователям. Вы можете использовать эту информацию при создании запросов.

В этом разделе приведены инструкции по выполнению SQL-запроса с помощью утилиты klsql2, а также пример такого запроса.

Вы также можете использовать любые другие приложения для работы с базами данных для создания SQL-запросов и представлений баз данных. Информация о том, как посмотреть параметры подключения к базе данных Kaspersky Security Center, например, имя инстанса и имя базы данных, приведена в соответствующем разделе.

Выполнение SQL-запроса с помощью утилиты klsql2

В этой статье приведены инструкции по использованию утилиты klsql2, а также по выполнению SQL-запроса с использованием этой утилиты.

Чтобы использовать утилиту klsql2:

1. Найдите утилиту klsql2 в папке установки Kaspersky Security Center. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. Не используйте версии утилиты klsql2, предназначенные для старых версий Kaspersky Security Center.

2. Создайте файл с расширением .sql в любом текстовом редакторе и поместите файл в одну папку с утилитой.

3. В созданном файле .sql введите требуемый SQL-запрос и сохраните файл.

4. На устройстве, на котором установлен Сервер администрирования Kaspersky Security Center, в командной строке введите следующую команду для выполнения SQL-запроса из файла .sql и сохранения результатов в файл result.xml:

   ```
   klsql2 -i src.sql -u <имя пользователя> -p <пароль> -o result.xml
   ```

   где `<имя пользователя>` и `<пароль>` являются учетными данными учетной записи пользователя, имеющего доступ к базе данных.

5. При необходимости введите имя учетной записи и пароль пользователя, имеющего доступ к базе данных.

6. Откройте созданные файлы result.xml и просмотрите результаты выполнения SQL-запроса.

Вы можете изменять файл .sql и создавать в нем любые SQL-запросы к публичным представлениям. Затем с помощью команды в командной строке можно запустить SQL-запрос и сохранить результаты в файл.

Пример SQL-запроса, созданного с помощью утилиты klsql2

В этом разделе приведен пример SQL-запроса, выполненного с помощью утилиты klsql2.

Следующие примеры показывают, как получить список событий, зарегистрированных на устройствах пользователей за последние семь дней, и отсортировать их по времени возникновения. Сначала отображаются самые последние события.

Пример для Microsoft SQL Server:

```
SELECT
  /* идентификатор события */
  e.nId,

  /* время возникновения события */
  e.tmRiseTime,

  /* внутреннее имя типа события  */
  e.strEventType,

  /* отображаемое имя события */
  e.wstrEventTypeDisplayName,

  /* отображаемое описание события */
  e.wstrDescription,

  /* имя группы, в которую входит устройство */
  e.wstrGroupName,

  /* отображаемое имя устройства, на котором произошло событие  */
  h.wstrDisplayName,
  CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

    /* IP-адрес устройства, на котором произошло событие */
  CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
  INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Пример для PostgreSQL:

```
SELECT
  /* идентификатор события */
  "e"."nId",

  /* время возникновения события */
  "e"."tmRiseTime",

  /* внутреннее имя типа события */
  "e"."strEventType",

  /* отображаемое имя события */
  "e"."wstrEventTypeDisplayName",

  /* отображаемое описание события */
  "e"."wstrDescription",

  /* отображаемое описание события */
  "e"."wstrGroupName",

  /* отображаемое имя устройства, на котором произошло событие */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* IP-адрес устройства, на котором произошло событие */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

Пример для MySQL или MariaDB:

```
SELECT

  /* идентификатор события */
  `e`.`nId`,

  /* время возникновения события */
  `e`.`tmRiseTime`,
```

```
  /* внутреннее имя типа события  */
  `e`.`strEventType`,

  /* отображаемое имя события */
  `e`.`wstrEventTypeDisplayName`,

  /* отображаемое описание события */
  `e`.`wstrDescription`,

  /* имя группы устройств */
  `e`.`wstrGroupName`,

  /* отображаемое имя устройства, на котором произошло событие  */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* IP-адрес устройства, на котором произошло событие */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Просмотр имени базы данных Kaspersky Security Center

Может быть полезно знать имя базы данных, если вам нужно, например, отправить SQL-запрос и подключиться к базе данных из редактора скриптов SQL.

Чтобы просмотреть имя базы данных Kaspersky Security Center:

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.

2. В окне свойств Сервера администрирования выберите раздел **Дополнительно**, а затем **Информация об используемой базе данных**.

3. В разделе **Информация об используемой базе данных** обратите внимание на следующие свойства базы данных (см. рис. ниже):

   - **Имя экземпляра**

     Имя экземпляра используемой базы данных Kaspersky Security Center. Значение по умолчанию – *.\KAV_CS_ADMIN_KIT*.

   - **Имя базы данных**

     Имя базы данных SQL Kaspersky Security Center. По умолчанию указано значение *KAV*.

   - **Место, выделенное под базу данных Kaspersky Security Center**

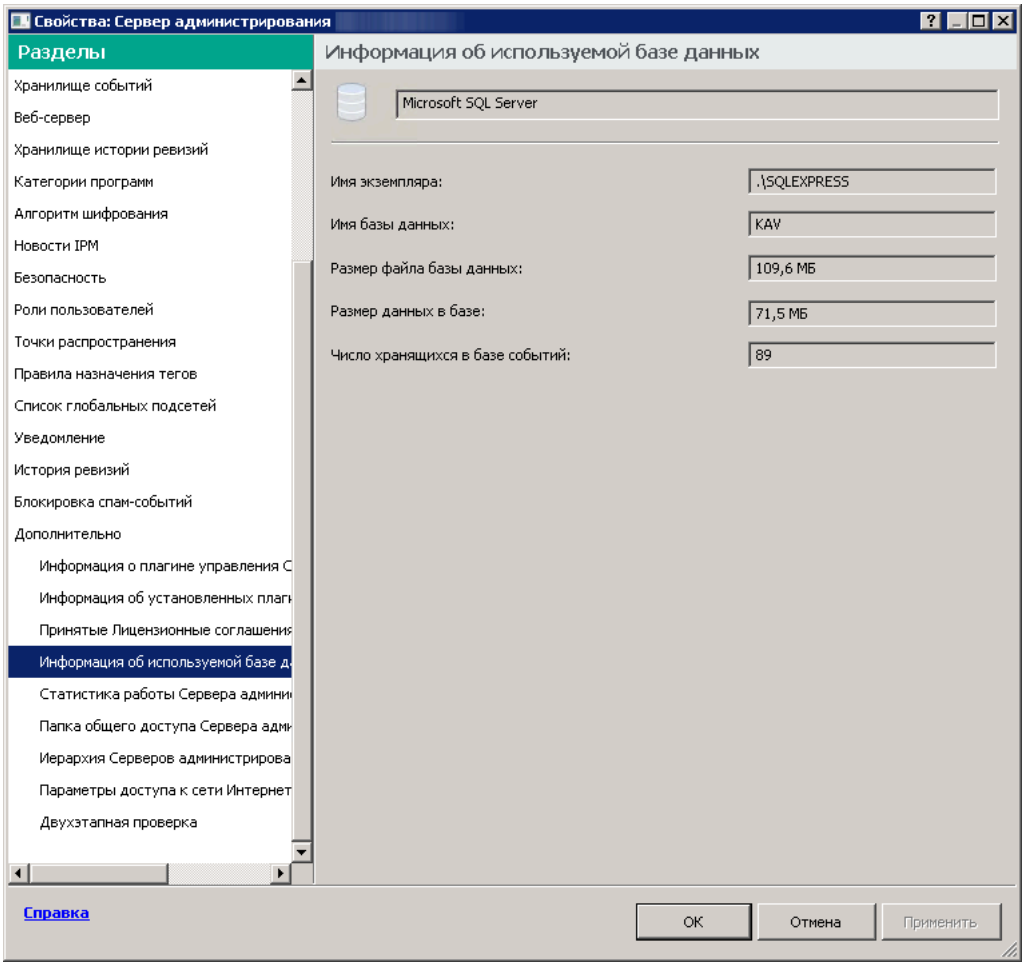
     Размер файла базы данных. Если вы хотите удалить ненужные данные, настройте сжатие базы данных с помощью задачи *Обслуживание Сервера администрирования*.

   - **Объем данных во всей базе данных**

     Фактический размер данных, используемых в настоящее время в СУБД. Подробную информацию о том как диагностировать СУБД см. в статье: Переполнение базы данных Kaspersky Security Center.

- **Число хранящихся в базе событий**

  Количество событий, хранящихся в настоящий момент в СУБД. Подробную информацию см. в статье: Обработка и хранение событий.



Раздел с информацией об используемой базе данных Сервера администрирования

4. Нажмите на кнопку **OK**, чтобы закрыть окно свойств Сервера администрирования.

Используйте это имя базы данных для подключения и обращения к базе данных в ваших SQL-запросах.

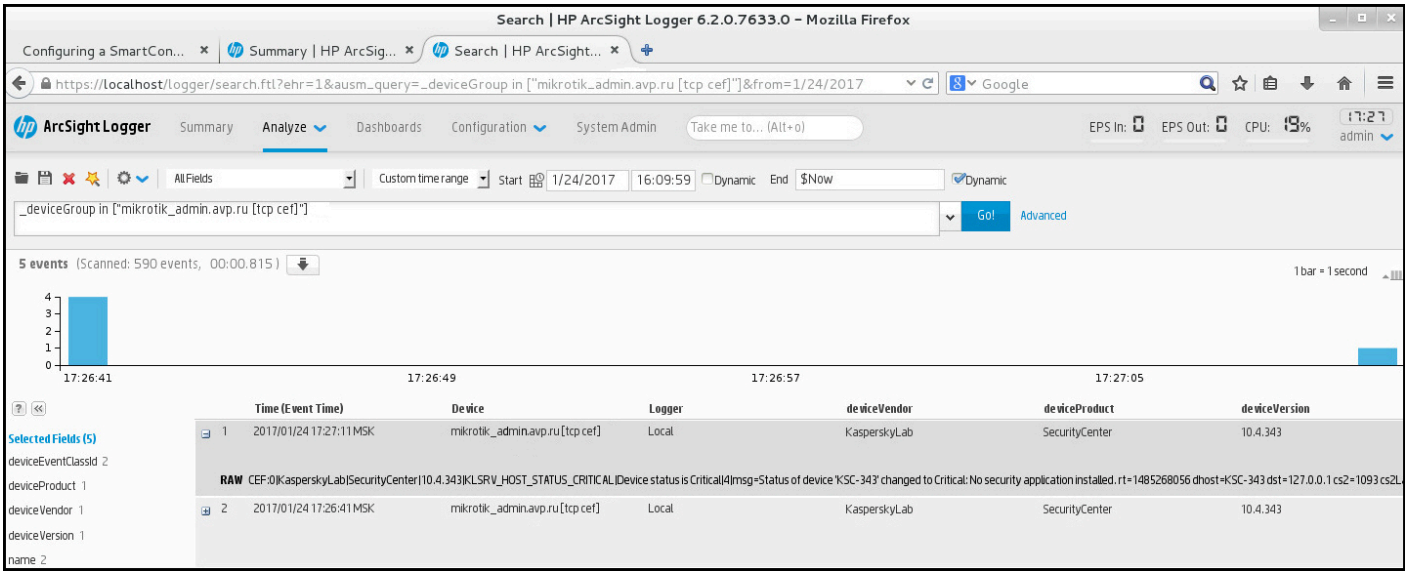
Просмотр результатов экспорта

Вы можете узнать, успешно ли завершилась процедура экспорта. Для этого проверьте, были ли получены SIEM-системой сообщения, содержащие экспортируемые события.

Если отправленные из Kaspersky Security Center события получены и правильно интерпретированы SIEM-системой, значит, настройка на обеих сторонах выполнена корректно. В противном случае проверьте и при необходимости исправьте настройки Kaspersky Security Center и SIEM-системы.

Ниже приведен пример событий, экспортированных в систему ArcSight. Например, первое событие – это критическое событие Сервера администрирования: *Статус устройства "Критический"*.

Отображение экспортированных событий зависит от используемой SIEM-системы.



Пример событий

Использование SNMP для отправки статистики приложениям сторонних производителей

В этом разделе описывается, как получить информацию от Сервера администрирования с помощью SNMP-протокола в Windows. Kaspersky Security Center содержит SNMP-агент, который передает статистику работы Сервера администрирования приложениям сторонних производителей с помощью OID.

В этом разделе также содержится информация о действиях для решения проблем, которые могут возникнуть при использовании SNMP для Kaspersky Security Center.

Настройка SNMP-службы для использования с Kaspersky Security Center

В этом разделе описано, как настроить SNMP-службу в Windows для получения информации от Сервера администрирования с помощью Simple Network Management Protocol (SNMP).

По умолчанию поддержка SNMP в Windows выключена.

Чтобы включить поддержку SNMP в Windows:

1. Перейдите в **Панель управления**.
2. Откройте меню **Установка и удаление приложений**.
3. Нажмите на **Включение или отключение компонентов Windows**.
4. В списке компонентов Windows перейдите к функции SNMP и нажмите на кнопку **OK**.
5. Перейдите в **Панель управления** → **Администрирование** → **Службы**.

6. Выберите **SNMP-службу** и запустите ее.

7. Проверьте, работает ли прослушивание, проверив его с помощью `netstat` для UDP-порта.

Поддержка SNMP в Windows включена.

Чтобы настроить SNMP-службу в Windows:

1. Убедитесь, что компонент **Агент SNMP** Kaspersky Security Center был установлен во время обычной или тихой установки.

2. Убедитесь, что **SNMP-служба** и **служба SNMP-ловушки** Windows запущены.

3. Убедитесь, что в вашей системе установлен MIB Browser ManageEngine.

4. В свойствах **SNMP-службы** на вкладке **Безопасность** добавьте два сообщества со следующими правами:

Сообщество	Права
`kaspersky`	`NOTIFY`
`public`	`READ WRITE`

5. В поле **Принимать SNMP-пакеты от этих устройств** добавьте IP-адрес устройства, на котором установлен ManageEngine MIB Browser, например 10.10.10.105.

6. На вкладке **Ловушки** введите `kaspersky` в поле **Имя сообщества**.

7. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно свойств службы.

8. В ManageEngine MIB Browser загрузите файл adminkit.mib из папки установки Kaspersky Security Center. По умолчанию файл adminkit.mib находится в папке <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center\snmp.

9. В поле **Устройство** окна ManageEngine MIB Browser, добавьте IP-адрес устройства, на котором установлен Сервер администрирования Kaspersky Security Center.

SNMP-служба настроен на получение информации от Сервера администрирования с помощью протокола Simple Network Management Protocol (SNMP).

SNMP-агент и идентификаторы объектов

Для Kaspersky Security Center SNMP-агент реализован в виде динамической библиотеки `klsnmpag.dll`, которая регистрируется установщиком при установке Сервера администрирования. SNMP-агент работает внутри процесса `snmp.exe` (который является сервисом Windows). Приложения сторонних производителей используют SNMP для получения статистики (которая представлена в виде счетчиков) производительности Сервера администрирования.

Каждый счетчик имеет уникальный *идентификатор объекта* (далее также OID, object identifier). Идентификатор объекта – это последовательность чисел, разделенных точками. Идентификаторы объектов Сервера администрирования начинаются с префикса 1.3.6.1.4.1.23668.1093. OID счетчика – это соединение этого префикса с суффиксом, описывающим счетчик. Например, счетчик со значением OID 1.3.6.1.4.1.23668.1093.1.1.4 имеет суффикс со значением 1.1.4.

Вы можете использовать SNMP-клиент (например, Zabbix) для контроля состояния вашей системы. Чтобы получить информацию, вы можете найти значение OID и ввести это значение в свой SNMP-клиент. Затем ваш SNMP-клиент вернет вам другое значение, которое характеризует состояние вашей системы.

Список счетчиков и типы счетчиков находятся в файле `adminkit.mib` на Сервере администрирования. *MIB* расшифровывается как Management Information Base. Вы можете импортировать и анализировать файлы `.mib` с помощью приложения MIB Viewer, которое предназначено для запроса и отображения значений счетчиков.

Получение имени счетчика строк из идентификатора объекта

Чтобы использовать идентификатор объекта (OID) для передачи информации приложениям сторонних производителей, вам может потребоваться получить имя счетчика строк из этого OID.

Чтобы получить имя счетчика строк из OID:

1. Откройте в текстовом редакторе файл `adminkit.mib`, расположенный на Сервере администрирования.
2. Найдите пространство имен, описывающее первое значение (слева направо).

   Например, для суффикса OID 1.1.4 это будет `"counters" (::= { kladminkit 1 })`.
3. Найдите пространство имен, описывающее второе значение.

   Например, для суффикса OID 1.1.4 это будет `counters 1`, что означает `deployment`.
4. Найдите пространство имен, описывающее третье значение.

   Например, для суффикса OID 1.1.4 это будет `deployment 4`, что означает `hostsWithAntivirus`.

Имя счетчика строк – это объединение этих значений, например, `<MIB base namespace>.counters.deployment.hostsWithAntivirus`, и это соответствует идентификатору OID со значением 1.3.6.1.4.1.23668.1093.1.1.4.

Значения идентификаторов объектов для SNMP

В таблице ниже приведены значения и описания идентификатора объекта (далее также OID), которые используются для передачи информации о производительности Сервера администрирования приложениям сторонних производителей.

Значение идентификатора объекта	Числовой тип данных	OID	Описание
deploymentStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.1.1	Статус развертывания. Статус может принимать одно из следующих значений: • **Информационное сообщение**. Лицензия больше не действует для N устройств. • **Предупреждение**. Одно из следующих: M устройств с установленными приложениями "Лаборатории Касперского" на N устройствах в группах Сервера администрирования (N > M). Срок действия лицензии L истекает на N устройствах через M дней. Задача T по установке приложений успешно завершена на N устройствах, для M устройств требуется перезагрузка. • **Критический**. Срок действия лицензии истек для N устройств. • **OK**. Ничего из вышеперечисленного.
noAntivirusSoftware	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.1	deploymentStatus – показывает, что в группах Сервера администрирования слишком много устройств, на которых не установлены управляемые приложения. Значение равно 1, если обнаружено нескольких устройств без управляемых приложений, и 0 в другом случае.
remoteInstallTaskFailed	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.2	deploymentStatus – показывает, что на некоторых устройствах не удалось выполнить задачу удаленной установки. Количество этих устройств можно получить с помощью hostsRemoteInstallFailed.
licenceExpiring	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.3	deploymentStatus – показывает, что есть несколько устройств, у которых истекает срок действия лицензии через семь дней. Количество этих устройств можно получить с помощью hostsLicenseExpiring.
licenceExpired	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.4	deploymentStatus – показывает, что есть несколько устройств, у которых срок действия лицензии истек. Вы можете узнать количество этих устройств с помощью hostsLicenseExpired.
hostsInGroups	Counter32	.1.3.6.1.4.1.23668.1093.1.1.3	Количество устройств в группах Сервера администрирования.
hostsWithAntivirus	Counter32	.1.3.6.1.4.1.23668.1093.1.1.4	Количество устройств в группах Сервера администрирования с установленными управляемыми приложениями.
hostsRemoteInstallFailed	Counter32	.1.3.6.1.4.1.23668.1093.1.1.5	Количество устройств, на которых не удалось выполнить задачу удаленной установки.
licenceExpiringSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.6	Идентификатор лицензионного ключа, срок действия которого истечет менее чем через семь дней.
licenceExpiredSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.7	Идентификатор лицензионного ключа, срок действия которого истек.
licenceExpiringDays	Unsigned32	.1.3.6.1.4.1.23668.1093.1.1.8	Количество дней до истечения срока действия лицензии. Для этого параметра срок действия лицензии истек, если до истечения срока его действия осталось менее 7 дней. Если до истечения срока действия осталось более 7 дней, значение равно 0.
hostsLicenceExpiring	Counter32	.1.3.6.1.4.1.23668.1093.1.1.9	Количество устройств с лицензией, срок действия которой истекает менее чем через семь дней.
hostsLicenceExpired	Counter32	.1.3.6.1.4.1.23668.1093.1.1.10	Количество устройств, у которых истек срок действия лицензии.

Значение идентификатора объекта	Числовой тип данных	OID	Описание
updatesStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.2.1	Состояние обновления антивирусных баз. Статус может принимать одно из следующих значений: • **Информационное сообщение**. Антивирусные базы на Сервере администрирования или на устройствах не обновлялись более одного дня; с момента установки приложения прошло менее одного дня. • **Предупреждение**. Антивирусные базы на Сервере администрирования или на устройствах не обновлялись более 3 дней. Это значение можно изменить в свойствах группы. • **Критический**. Антивирусные базы на Сервере администрирования или на устройствах не обновлялись более 7 дней. Это значение можно изменить в свойствах группы. • **OK**. Ничего из вышеперечисленного.
serverNotUpdated	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.1	Давно не выполнялась полная проверка Сервера администрирования. Время, которое считается долгим, указывается в updatesStatus.
notUpdatedHosts	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.2	Некоторые устройства не обновлялись в течение долгого времени (по умолчанию **Критическое** – семь дней и более, **Предупреждение** – три дня). Вы можете узнать количество этих устройств с помощью hostsNotUpdated.
lastServerUpdateTime	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.2.3	Дата последнего обновления антивирусных баз на Сервере администрирования.
hostsNotUpdated	Counter32	.1.3.6.1.4.1.23668.1093.1.2.4	Количество устройств, содержащих антивирусные базы, которые давно не обновлялись (по умолчанию **Критическое** – семь дней и более, **Предупреждение** – три дня). Если есть устройства со статусом обновления **Критическое**, учитываются только эти устройства. Вы можете получить статус обновления с помощью updatesStatus.
protectionStatus	INTEGER { ok(0), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.3.1	Статус постоянной защиты. Одно из следующих: • **Предупреждение**. Одно из следующих: На устройстве, входящем в группу Сервера администрирования, обнаружено нарушение безопасности. Из-за ошибок шифрования некоторые устройства изменили состояние защиты. Полная проверка давно не выполнялась. • **Критический**. На некоторых устройствах в группах Сервера администрирования не работает антивирусная защита. • **OK**. Ничего из вышеперечисленного.
antivirusNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.1	Приложение безопасности не работает на некоторых устройствах. Вы можете узнать количество этих устройств с помощью hostsAntivirusNotRunning.
realtimeNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.2	Постоянная защита не работает на некоторых устройствах. Вы можете узнать количество этих устройств с помощью hostsRealtimeNotRunning.
psRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.2.3	Количество устройств, уровень постоянной защиты которых отличается от уровня, установленного администратором
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.4	Есть устройства с не вылеченными объектами. Вы можете узнать количество этих устройств с помощью hostsNotCuredObject.
tooManyThreats	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.5	Есть устройствах, на которых обнаружены угрозы. Вы можете узнать количество этих устройств с помощью hostsTooManyThreats.

Значение идентификатора объекта	Числовой тип данных	OID	Описание
virusOutbreak	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.6	Статус вирусной атаки системы. Значение равно 1, если определенное количество вирусов было обнаружено в течение определенного времени, и 0 в других случаях. Количество вирусов и время указывается на Сервере администрирования с помощью параметра `Вирусная атака`.
psVulnerabilitiesFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.7	Обнаружены уязвимости.
psEncryptionFaultsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.8	Обнаружены ошибки шифрования, изменившие состояние защиты устройства.
psVulnerableHostsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.9	На некоторых устройствах обнаружены уязвимости.
psNotScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.10	Обнаружены устройства, на которых не выполнялась полная проверка в течение длительного времени.
psNagentsNotRunningUntilReboot	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.11	Обнаружены устройства, на которых Агент администрирования запускается только после перезагрузки.
hostsAntivirusNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.3	Количество устройств, на которых не запущены приложения безопасности.
hostsRealtimeNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.4	Количество устройств, на которых не запущена постоянная защита.
hostsRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.5	Количество устройств с недопустимым уровнем постоянной защиты.
hostsNotCuredObject	Counter32	.1.3.6.1.4.1.23668.1093.1.3.6	Количество устройств с не вылеченными объектами.
hostsTooManyThreats	Counter32	.1.3.6.1.4.1.23668.1093.1.3.7	Количество устройств, которые содержат угрозы.
fullscanStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.4.1	Статус полной проверки может быть одним из следующих: • **Информационное сообщение**. С момента установки приложения прошло менее 7 дней. • **Предупреждение**. Полная проверка не производилась более 7 дней с момента установки приложения. • **Критический**. Полная проверка не производилась более 14 дней с момента установки приложения. • **OK**. Ничего из вышеперечисленного.
notScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.4.2.1	Есть несколько устройств, на которых не выполнялась проверка в течение определенного времени. Вы можете узнать количество этих устройств с помощью `hostsNotScannedLately`. Время указывается в `fullScanStatus`.
hostsNotScannedLately	Counter32	.1.3.6.1.4.1.23668.1093.1.4.3	Количество устройств, на которых не выполнялась проверка в течение определенного времени. Время указывается в `fullScanStatus`.

Значение идентификатора объекта	Числовой тип данных	OID	Описание
logicalNetworkStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.5.1	Состояние логической сети Сервера администрирования. Одно из следующих: • **Предупреждение**. Если есть устройства со статусом Предупреждение, к которым нет доступа, или если есть устройства, которые не принадлежат ни к какой группе Сервера администрирования. • **Критический**. Если есть устройства, контроль над которыми потерян Сервером администрирования, или есть устройства со статусом Критический, к которым нет доступа. • **OK**. Ничего из вышеперечисленного.
notConnectedLongTime	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.1	Есть несколько устройств, которые в течение долгого времени не были подключены к Серверу администрирования (семь дней и более для устройства со статусом **Предупреждение** и четыре дня для устройства со статусом **Критический**). Вы можете узнать количество этих устройств с помощью hostsNotConnectedLongTime.
controlLost	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.2	Есть устройства, контроль над которыми потерян Сервером администрирования. Вы можете узнать количество этих устройств с помощью hostsControlLost.
hostsFound	Counter32	.1.3.6.1.4.1.23668.1093.1.5.3	Количество обнаруженных Сервером администрирования устройств, не входящих ни в одну группу Сервера администрирования.
groupsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.5.4	Количество групп Сервера администрирования.
hostsNotConnectedLongTime	Counter32	.1.3.6.1.4.1.23668.1093.1.5.5	Количество устройств, которые долгое время не подключались к Серверу администрирования. Время, которое считается долгим, указывается в notConnectedLongTime.
hostsControlLost	Counter32	.1.3.6.1.4.1.23668.1093.1.5.6	Количество устройств, которые не контролируются Сервером администрирования.
eventsStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.6.1	Статус событий подсистемы может быть одним из следующих: • **Предупреждение**. Одно из следующих: Устройства групп Сервера администрирования давно не выполняли поиск обновлений Windows. Есть устройства с проблемами, связанные со статусом. • **Критический**. Одно из следующих: Хотя бы на одном устройстве произошло критическое событие. Хотя бы на одном устройстве произошло событие отказа функционирования. Есть событие неудачного завершения задачи хотя бы на одном устройстве. Устройства групп Сервера администрирования давно не выполняли поиск обновлений Windows. Есть устройства с проблемами, связанные со статусом. • **Информационное сообщение.** Одно из следующих: С момента последней полной антивирусной проверки на всех устройствах прошло меньше недели. Задачи удаленной установки выполнены и ни одно устройство не требует перезагрузки. Последнее обновление Сервера администрирования выполнялось меньше недели назад. Сервер администрирования давно не обновлялся, но в сейчас выполняется обновление. • **OK**. Ничего из вышеперечисленного.

Значение идентификатора объекта	Числовой тип данных	OID	Описание
`criticalEventOccured`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.6.2.1	`eventsStatus` – показывает, что на Сервере администрирования произошли критические события. Вы можете получить количество этих событий с помощью `criticalEventsCount`. Значение равно 1, если есть хотя бы одно критическое событие на любом устройстве, и 0 в другом случае.
`criticalEventsCount`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.6.3	Количество критических событий на Сервере администрирования.

Устранение неисправностей

В этом разделе перечислены решения нескольких типичных проблем, с которыми вы можете столкнуться при использовании SNMP-службы.

Приложение стороннего производителя не может подключиться к SNMP-службе

Убедитесь, что SNMP-служба установлена и настроена, как описано в разделе Настройка SNMP-службы для использования с Kaspersky Security Center.

SNMP-служба работает, но приложение стороннего производителя не может получить никаких значений

Разрешите трассировку SNMP-агента и убедитесь, что создан непустой файл. Это означает, что SNMP-агент зарегистрирован правильно и работает. После этого разрешите подключения от SNMP-службы в параметрах службы. Если служба работает на том же устройстве, что и SNMP-агент, список IP-адресов должен содержать либо IP-адрес этого устройства, либо `loopback 127.0.0.1`.

В Windows должна работать SNMP-служба, которая взаимодействует с агентами. Вы можете указать пути к SNMP-агентам в реестре Windows с помощью regedit.

- Для Windows 10:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents
- Для Windows Vista и Windows Server 2008:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SNMP\Parameters\ExtensionAgents

Вы также можете разрешить трассировку SNMP-агента с помощью regedit.

- для 32-разрядной системы:
  HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug
- для 64-разрядной системы:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Deb
  "TraceLevel"=dword:00000004

"TraceDir"="C:\\"

Значения не соответствуют статусам Консоли администрирования

Для снижения нагрузки на Сервер администрирования реализовано кеширование значений для SNMP-агента. Задержка между актуализацией кеша и изменяемыми значениями на Сервере администрирования может вызвать несоответствие между значениями, возвращаемыми SNMP-агентом, и фактическими. При работе с приложениями сторонних производителей следует учитывать возможную задержку.

Работа в облачном окружении

В этом разделе представлена информация о развертывании и обслуживании Kaspersky Security Center в облачных окружениях, таких как Amazon Web Services, Microsoft Azure и Google Cloud.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky Security Center.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

О работе в облачном окружении

Kaspersky Security Center 15.1 не только работает с физическими устройствами, но также предоставляет специальные возможности для работы в облачном окружении. Kaspersky Security Center работает со следующими виртуальными машинами:

- Инстансы Amazon EC2 (далее также *инстансы*). Инстанс Amazon EC2 это виртуальная машина, которая создана на основе платформы Amazon Web Services (AWS). Kaspersky Security Center использует AWS *API* (Application Programming Interface, программный интерфейс приложения).
- Виртуальные машины Microsoft Azure. Kaspersky Security Center использует API Azure.
- Инстансы виртуальных машин Google Cloud. Kaspersky Security Center использует API Google.

Вы можете развернуть Kaspersky Security Center на инстансе или на виртуальной машине для управления защитой устройств в облачном окружении и пользоваться специальными возможностями Kaspersky Security Center для работы в облачном окружении. Эти возможности включают:

- опрос инстансов, находящихся в облачном окружении, средствами API;
- использование инструментов API для установки Агента администрирования и приложений безопасности на устройствах в облачном окружении;
- поиск устройств по признаку принадлежности к определенному облачному сегменту.

Вы также можете использовать инстанс или виртуальную машину, на которых развернут Сервер администрирования Kaspersky Security Center, для защиты физических устройств (например, если такой облачный сервер оказывается выгоднее в обслуживании и содержании, чем физический). В этом случае работа с Сервером администрирования будет устроена так же, как если бы Сервер администрирования был установлен на физическом устройстве.

В Kaspersky Security Center, развернутом с платного Amazon Machine Image (AMI) (в AWS) или используемом на основе подписки с ежемесячной тарификацией в зависимости от объема услуг (в Azure), возможности Системного администрирования активируются автоматически, но Управление мобильными устройствами не может быть активировано.

Сервер администрирования устанавливается совместно с Консолью администрирования. Kaspersky Security для Windows Server также автоматически устанавливается на устройство, на котором установлен Сервер администрирования.

Вы можете настроить Kaspersky Security Center, используя мастер настройки облачного окружения, с учетом специфики работы в облачном окружении.

Сценарий: развертывание в облачном окружении

В этом разделе описан сценарий развертывания Kaspersky Security Center для работы в облачном окружении, таком как Amazon Web Services, Microsoft Azure и Google Cloud.

После завершения сценария развертывания Сервер администрирования Kaspersky Security Center и Консоль администрирования будут запущены и настроены с параметрами по умолчанию. На выбранных инстансах Amazon EC2 или виртуальных машинах Microsoft Azure будет развернута антивирусная защита под управлением Kaspersky Security Center. В дальнейшем вы можете настраивать Kaspersky Security Center более подробно, создавать сложную структуру групп администрирования, создавать для групп различные политики и задачи.

Развертывание Kaspersky Security Center для работы в облачных окружениях состоит из следующих шагов:

1. Подготовка.
2. Развертывание Сервера администрирования.
3. Установка антивирусных приложений "Лаборатории Касперского" на виртуальные устройства, которые необходимо защитить.
4. Настройка параметров загрузки обновлений.
5. Настройка параметров работы с отчетами о состоянии защиты устройств.

Для первоначальной настройки существует мастер настройки облачного окружения. Мастер запускается автоматически при первом развертывании Kaspersky Security Center из готового образа. Вы можете запустить мастер в любой момент. Также вы можете самостоятельно выполнить все действия, которые выполняет мастер.

Рекомендуется отвести на развертывание Сервера администрирования Kaspersky Security Center в облачном окружении не менее часа, а всего на развертывание защиты в облачном окружении – не менее одного рабочего дня.

Развертывание Kaspersky Security Center в облачном окружении состоит из следующих этапов:

1. **Планирование конфигурации облачных сегментов**

   Ознакомьтесь с работой Kaspersky Security Center в облачном окружении. Спланируйте, где будет развернут Сервер администрирования (внутри или вне облачного окружения); определите сколько облачных сегментов вы планируете защищать. Если вы планируете разместить Сервер администрирования вне облачного окружения, либо если вы планируете защищать более 5000 устройств, то вам потребуется установить Сервер администрирования вручную.

   Для работы с Google Cloud Сервер администрирования можно установить только вручную.

2. **Планирование ресурсов**

   Убедитесь, что выполнены все условия, необходимые для развертывания.

3. **Подписка на Kaspersky Security Center в виде готового образа**

   Выберите один из готовых образов AMI в магазине AWS Marketplace или выберите использование ежемесячных счетов за использование SKU в магазине Azure Marketplace, оплатите в соответствии с правилами магазина, если необходимо (или используйте модель BYOL), и используйте образ для развертывания инстанса Amazon EC2 или виртуальной машины Microsoft Azure с установленным приложением Kaspersky Security Center.

   Этот этап необходим, только если вы планируете разместить Сервер администрирования на инстансе или виртуальной машине внутри облачного окружения и при этом планируете разворачивать защиту не более чем 5000 устройств. Иначе этот этап не нужен, и вместо него вам нужно вручную установить Сервер администрирования, Консоль администрирования и СУБД.

   Этот шаг недоступен для Google Cloud.

4. **Определение местоположения СУБД**

   Определение, где будет расположена СУБД.

   Если вы планируете использовать базу данных вне облачного окружения, убедитесь, что у вас есть рабочая база данных.

   Если вы планируете использовать Amazon Relational Database Service (RDS), создайте базу данных с RDS в облачном окружении AWS.

   Если вы планируете использовать СУБД Microsoft Azure SQL, создайте базу данных со службой базы данных Azure в облачном окружении Microsoft Azure.

   Если вы планируете использовать Google MySQL, создайте базу данных в Google Cloud (подробнее см. в документации https://cloud.google.com/sql/docs/mysql).

5. **Установка Сервера администрирования и Консоли администрирования (на основе Microsoft Management Console и/или Консоли на основе веб-интерфейса) на выбранных устройствах вручную**

   Установите Сервер администрирования, Консоль администрирования и СУБД на выбранные устройства так, как описано в основном сценарии установки Kaspersky Security Center.

   Этот этап необходим, если вы планируете разместить Сервер администрирования вне облачного окружения или если вы планируете разворачивать защиту более чем 5000 устройств. Затем убедитесь, что ваш Сервер администрирования соответствует требованиям к оборудованию. Иначе этот этап не нужен и достаточно подписки на Kaspersky Security Center в виде готового образа в магазине AWS Marketplace, в магазине Azure Marketplace или в Google Cloud.

6. **Обеспечение прав для работы Сервера администрирования с облачными-службами API**

   В AWS перейдите в Консоль управления AWS и создайте IAM-роль или учетную запись IAM-пользователя. Созданная IAM-роль (либо учетная запись IAM-пользователя) позволит Kaspersky Security Center работать с AWS API: опрашивать облачные сегменты и разворачивать защиту.

В Azure, создайте подписку и ИД приложения с паролем. Kaspersky Security Center использует эти учетные данные для работы в Azure API: опрашивать облачные сегменты и разворачивать защиту.

В Google Cloud зарегистрируйте проект, получите идентификатор проекта и закрытый ключ. Kaspersky Security Center использует эти учетные данные для опроса облачных сегментов с помощью Google API.

7. **Создание IAM-роли для защищаемых инстансов (только для AWS)**

   Создайте в Консоли управления AWS IAM-роль, которая определяет набор разрешений для выполнения запросов к AWS. Созданную роль вы впоследствии будете назначать новым инстансам. IAM-роль нужна для установки приложений на инстансы с помощью Kaspersky Security Center.

8. **Подготовка базы данных с помощью Amazon Relational Database Service или Microsoft Azure SQL**

   Если вы планируете использовать базу данных Amazon Relational Database Service (RDS), создайте инстанс базы данных Amazon RDS и корзина S3, где будет храниться резервная копия базы данных. Вы можете пропустить этот этап, если вам нужна база данных на том же экземпляре EC2, где установлен Сервер администрирования, или если вы хотите, чтобы ваша база данных находилась в другом месте.

   Если вы планируете использовать Microsoft Azure SQL, создайте учетную запись хранилища и базу данных в Microsoft Azure.

   Если вы планируете использовать Google MySQL, создайте базу данных в Google Cloud (подробнее см. в документации https://cloud.google.com/sql/docs/mysql).

9. **Лицензирование Kaspersky Security Center для работы в облачном окружении**

   Убедитесь, что у вас есть лицензия для работы Kaspersky Security Center в облачном окружении, и предоставьте код активации либо файл ключа, чтобы приложение добавило его в хранилище лицензий. Этот этап может быть завершен во время настройки облачного окружения.

   Этот этап обязателен, если вы используете Kaspersky Security Center, установленный из бесплатного готового образа AMI по модели BYOL, или если вы устанавливаете Kaspersky Security Center самостоятельно без использования образов AMI. В каждом из этих случаев для активации Kaspersky Security Center вам нужна лицензия на приложение Kaspersky Security для виртуальных сред или на приложение Kaspersky Security для виртуальных и облачных сред.

   Если вы используете Kaspersky Security Center, установленный из готового образа, то этот этап является необязательным и соответствующее окно мастера настройки облачного окружения не отображается.

10. **Аутентификация в облачном окружении**

    Укажите в Kaspersky Security Center ваши учетные данные AWS, Azure или Google Cloud, чтобы Kaspersky Security Center мог работать с необходимыми разрешениями. Этот этап может быть завершен во время авторизации в облачном окружении.

11. **Получение Сервером администрирования сведений об устройствах в облачном сегменте путем опроса облачного сегмента**

    Запустите опрос облачного сегмента. В облачном окружении AWS Kaspersky Security Center получит адреса и имена всех инстансов, доступ к которым обеспечивают права IAM-роли или права IAM-пользователя. В облачном окружении Microsoft Azure Kaspersky Security Center получит адреса и имена всех виртуальных машин, доступ к которым обеспечивают права роли Читатель.

    В дальнейшем вы можете с помощью Kaspersky Security Center устанавливать приложения "Лаборатории Касперского" и других производителей на обнаруженные инстансы или виртуальные машины.

    Kaspersky Security Center запускает опрос регулярно, поэтому, если появятся новые инстансы или виртуальные машины, то они будут обнаружены автоматически.

12. **Объединение всех устройств сети в группу администрирования Cloud**

    Переместите все обнаруженные инстансы или виртуальные машины в группу администрирования **Управляемые устройства\Cloud**, чтобы они стали доступными для централизованного управления. Если вы хотите разбить устройства на подгруппы, например, в зависимости от того, какая операционная система на них установлена, вы можете создать несколько групп администрирования внутри группы **Управляемые устройства\Cloud**. Вы можете настроить автоматическое перемещение всех устройств, которые будут обнаружены во время регулярных опросов, в группу **Управляемые устройства\Cloud**.

13. **Связь устройств в сети с Сервером администрирования с помощью Агента администрирования**

    Установите Агента администрирования на устройствах в облачном окружении. Компонент Kaspersky Security Center обеспечивает связь устройства с Сервером администрирования. Параметры Агента администрирования автоматически настраиваются по умолчанию.

    Вы можете установить Агент администрирования на каждое устройство локально. Вы также можете установить Агент администрирования на устройства удаленно, с помощью Kaspersky Security Center. Или вы можете пропустить этот этап и установить Агент администрирования вместе с последними версиями приложений безопасности.

14. **Установка последних версий приложений безопасности на устройства сети**

    Выберите устройства, на которые вы хотите установить приложения безопасности, и установите на эти устройства последние версии приложений безопасности. Вы можете произвести установку либо удаленно, с помощью Kaspersky Security Center на Сервере администрирования, либо локально.

    Возможно, вам придется создать инсталляционные пакеты для этих приложений вручную.

    Для инстансов и виртуальных машин под управлением Linux предназначено приложение Kaspersky Endpoint Security для Linux.

    Для инстансов и виртуальных машин под управлением Windows предназначено приложение Kaspersky Security для Windows Server.

15. **Настройка параметров обновлений**

Задача **Поиск уязвимостей и требуемых обновлений** создается автоматически при запуске настройки облачного окружения. Вы также можете создать ее вручную. Эта задача обеспечивает автоматический поиск и загрузку необходимых обновлений приложений для последующей установки на устройства в сети средствами Kaspersky Security Center.

После завершения настройки облачной среды рекомендуется выполнить следующий этап:

1. **Настройка работы с отчетами**

    Вы можете просматривать отчеты на вкладке **Мониторинг** в рабочей области узла **Сервер администрирования**. Вы можете получать отчеты по электронной почте. Отчеты на вкладке **Мониторинг** доступны по умолчанию. Чтобы настроить получение отчетов по электронной почте, укажите адреса электронной почты, на которые будут приходить отчеты, и настройте формат отчетов.

Результаты

После завершения сценария вы можете убедиться, что первоначальная настройка прошла успешно:

- Вы можете подключиться к Серверу администрирования с помощью Консоли администрирования или с помощью Kaspersky Security Center Web Console.
- На управляемых устройствах установлены и работают последние версии приложений безопасности "Лаборатории Касперского".
- Kaspersky Security Center создал для всех управляемых устройств политики и задачи по умолчанию.

Предварительные условия для развертывания Kaspersky Security Center в облачном окружении

Перед началом развертывания Kaspersky Security Center в облачном окружении, таком как Amazon Web Services или Microsoft Azure, убедитесь, что у вас имеется:

- доступ в интернет;
- одна из следующих учетных записей:
  - учетная запись Amazon Web Services (для работы с AWS);
  - учетная запись Microsoft (для работы с Azure);
  - учетная запись Google (для работы с Google Cloud).
- Одно из следующих:
  - лицензия на Kaspersky Security для виртуальных сред;
  - лицензия на Kaspersky Security для виртуальных и облачных сред;
  - средства на приобретение такой лицензии (Kaspersky Security для виртуальных сред или Kaspersky Security для виртуальных и облачных сред);
  - средства на оплату в магазине Azure Marketplace готового образа.
- руководства к последним версиям приложений Kaspersky Endpoint Security для Linux и Kaspersky Security для Windows Server.

Аппаратные требования для Сервера администрирования в облачном окружении

Для развертывания в облачных окружениях требования к Серверу администрирования и серверу базы данных такие же, как и к физическому Серверу администрирования (в зависимости от того, каким количеством устройств вы хотите управлять). Дополнительную информацию см. в документации к облачному окружению.

Варианты лицензирования в облачном окружении

Работа в облачном окружении не входит в базовую функциональность Kaspersky Security Center и требует лицензии.

В Kaspersky Security Center доступно два варианта лицензирования для работы в облачном окружении:

- Платный образ AMI (в Amazon Web Services) или использование ежемесячных счетов за использование SKU (в Microsoft Azure).

  Такой вариант лицензирования Kaspersky Security Center предоставляет также лицензию для Kaspersky Endpoint Security для Linux и Kaspersky Security для Windows Server. Платить нужно в соответствии с правилами используемого облачного окружения.

  Эта модель позволяет вам управлять не более чем 200 клиентскими устройствами для одного Сервера администрирования.

- Готовый бесплатный образ с использованием собственной лицензии по модели BYOL (Bring Your Own License).

  Для лицензирования Kaspersky Security Center в AWS или Azure необходима лицензия на использование одного из приложений:

  - Kaspersky Security для виртуальных сред
  - Kaspersky Security для виртуальных и облачных сред

  Эта модель позволяет вам управлять до 100 000 клиентских устройств для одного Сервера администрирования. Эта модель также позволяет вам управлять устройствами вне облачного окружения AWS, Azure или Google.

  Вы можете выбрать модель BYOL в любом из следующих случаев:

  - у вас уже есть действующая лицензия на Kaspersky Security для виртуальных сред;
  - у вас уже есть действующая лицензия на Kaspersky Security для виртуальных и облачных сред;
  - вы хотите приобрести лицензию непосредственно перед развертыванием Kaspersky Security Center.

  На этапе первоначальной настройки Kaspersky Security Center запрашивает у вас код активации или файл ключа.

  При выборе BYOL вам не нужно будет оплачивать использование Kaspersky Security Center через магазин Azure Marketplace или AWS Marketplace.

В обоих случаях возможности Системного администрирования активируются автоматически, но Управление мобильными устройствами не может быть активировано.

Если возникает ошибка при попытке активировать функцию Поддержка облачного окружения с использованием лицензии Kaspersky Security для виртуальных и облачных сред, используйте файл ключа.

После подписки на Kaspersky Security Center вы получаете Amazon Elastic Compute Cloud (Amazon EC2) или виртуальную машину Microsoft Azure с Сервером администрирования Kaspersky Security Center. Инсталляционные пакеты Kaspersky Security для Windows Server и Kaspersky Endpoint Security для Linux доступны на Сервере администрирования. Вы можете установить эти приложения на устройствах в облачном окружении. Вам не нужно активировать эти приложения по лицензии.

Если управляемое устройство не видимо в сети Сервера администрирования более недели, приложение безопасности (Kaspersky Security для Windows Server или Kaspersky Endpoint Security для Linux) на этом устройстве перейдет в режим ограниченной функциональности. Чтобы активировать приложение снова, вам нужно сделать устройство, на котором установлено приложение безопасности, видимым в сети Сервера администрирования снова.

Параметры базы данных для работы в облачном окружении

У вас должна быть база данных для работы с Kaspersky Security Center. При развертывании Kaspersky Security Center в AWS, в Microsoft Azure или Google Cloud у вас есть три параметра:

- Создайте локальную базу данных на одном устройстве с Сервером администрирования. Kaspersky Security Center поставляется вместе с базой данных SQL Server Express, которая может поддерживать до 5000 управляемых устройств. Выберите этот параметр, если базы данных SQL Server Express Edition достаточно для ваших потребностей.

- Создайте базу данных с Relational Database Service (RDS) в облачном окружении AWS или с сервисом базы данных Azure в облачном окружении Microsoft Azure. Выберите этот параметр, если вы хотите использовать СУБД, отличную от SQL Express. Ваши данные будут перенесены внутри облачного окружения, где они останутся, и у вас не будет никаких дополнительных затрат. Если вы уже работаете с Kaspersky Security Center локально и имеете некоторые данные в своей базе данных, вы можете перенести свои данные в новую базу данных.

  Для работы на платформе Google Cloud можно использовать только Cloud SQL для MySQL.

- Используйте существующий сервер базы данных. Выберите этот параметр, если вы уже используете сервер базы данных и хотите использовать его для Kaspersky Security Center. Если этот сервер расположен все облачного окружения, ваши данные будут перенесены через интернет, что может привести к дополнительным расходам.

Процедура развертывания Kaspersky Security Center в облачном окружении имеет специфические шаги для создания (выбора) базы данных.

Работа в облачном окружении Amazon Web Services

В этом разделе описано, как подготовиться к работе с Kaspersky Security Center в Amazon Web Services.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky Security Center.

О работе в облачном окружении Amazon Web Services

Вы можете приобрести Kaspersky Security Center в магазине приложений AWS Marketplace в виде образа AMI (Amazon Machine Image) – готового образа предварительно настроенной виртуальной машины. Вы можете подписаться на платный готовый образ AMI или BYOL AMI и на основе этого образа создать инстанс Amazon EC2 с установленным Сервером администрирования Kaspersky Security Center.

Для работы с платформой AWS, и в частности для того, чтобы приобретать приложения в AWS Marketplace и 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.

Если вы подписались на образ AMI, доступный в магазине приложений AWS Marketplace, то вы получаете инстанс с готовым к работе Kaspersky Security Center. Вам не нужно устанавливать приложение самостоятельно. Сервер администрирования Kaspersky Security Center в этом случае устанавливается на инстанс без вашего участия. После установки вы можете запустить Консоль администрирования и подключиться к Серверу администрирования, чтобы начать работу с Kaspersky Security Center.

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.

Создание IAM-роли и учетных записей IAM-пользователя для инстансов Amazon EC2

В этом разделе описано, какие действия необходимо выполнить, чтобы обеспечить корректную работу Сервера администрирования. Эти действия включают работу с сервисами AWS, с IAM-ролями (Identity and Access Management) и учетными записями пользователей. Также описано, какие действия должны быть выполнены с клиентскими устройствами, чтобы установить на них Агент администрирования и затем защитные приложения Kaspersky Security для Windows Server и Kaspersky Endpoint Security для Linux.

Обеспечение прав для работы Сервера администрирования Kaspersky Security Center с AWS

Стандарты работы в облачном окружении Amazon Web Services рекомендуют, чтобы специальная IAM-роль была назначена экземпляру Сервера администрирования для работы с сервисами AWS. Создайте в консоли AWS IAM-роль, которая определяет набор разрешений для выполнения запросов к сервисам AWS. IAM-роль обеспечивает права на опрос облачных сегментов и на установку приложений на инстансы.

После того как вы создадите IAM-роль и назначите ее на Сервер администрирования, вы сможете разворачивать защиту инстансов, пользуясь этой ролью и не предоставляя Kaspersky Security Center никакой дополнительной информации.

Однако в следующих случаях может быть целесообразно отказаться от создания IAM-роли для Сервера администрирования:

- Если устройства, защитой которых вы планируете управлять, являются инстансами EC2 внутри облачного окружения Amazon Web Services, а Сервер администрирования находится вне него.

- Если вы планируете управлять защитой инстансов не только внутри вашего облачного сегмента, но и внутри других облачных сегментов, созданных под другой учетной записью в AWS. В таком случае вам понадобится IAM-роль только для защиты вашего облачного сегмента. Для защиты другого облачного сегмента IAM-роль не понадобится.

В этих случаях вам потребуется создать не IAM-роль, а *учетную запись IAM-пользователя*, от имени которого Kaspersky Security Center будет работать 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-роли либо IAM-пользователя требуется Консоль управления AWS. Для работы с Консолью управления AWS вам понадобятся имя пользователя и пароль от учетной записи в AWS.

Создание IAM-роли для Сервера администрирования

Прежде чем разворачивать Сервер администрирования, создайте в Консоли управления AWS IAM-роль с необходимыми правами для установки приложений на инстансы. Подробнее см. в справке AWS в разделах об IAM-ролях.

Чтобы создать IAM-роль для Сервера администрирования:

1. Откройте Консоль управления AWS и выполните вход под своей учетной записью AWS.

2. В разделе **Роли** создайте роль со следующими правами:

   - **AmazonEC2ReadOnlyAccess**, если вы планируете только запускать опрос облачных сегментов и не планируете устанавливать приложения на инстансы EC2 с помощью AWS API.

   - **AmazonEC2ReadOnlyAccess** и **AmazonSSMFullAccess**, если вы планируете и запускать опрос облачных сегментов, и устанавливать приложения на инстансы EC2 с помощью AWS API. В этом случае вам понадобится также назначить на защищаемые инстансы EC2 IAM-роль с правами AmazonEC2RoleforSSM.

Вам потребуется назначить эту роль на инстанс EC2, который вы будете использовать в качестве Сервера администрирования.

Созданная роль доступна для всех приложений на Сервере администрирования. Поэтому любое приложение, работающее на Сервере администрирования, имеет возможность опрашивать облачные сегменты либо устанавливать приложения на инстансы EC2 внутри облачного сегмента.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky Security Center.

Создание учетной записи IAM-пользователя для работы Kaspersky Security Center

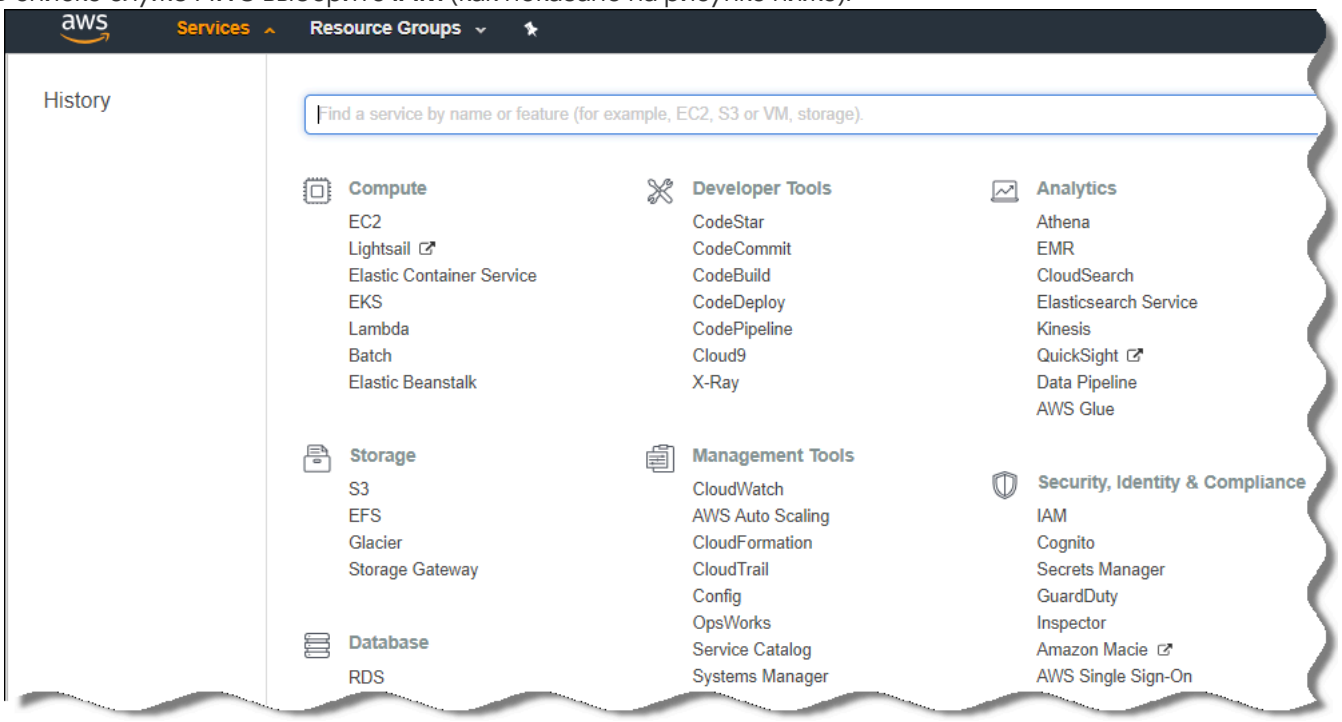
Учетная запись IAM-пользователя необходима для работы с Kaspersky Security Center, если Серверу администрирования не назначена IAM-роль с правами на обнаружение устройств и установку приложений на инстансы. Эта же учетная запись или другая учетная запись также требуется для резервного копирования задачи данных Сервера администрирования, если вы используете корзину S3. 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 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:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html;
- http://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** (как показано на рисунке ниже).



Список сервисов в AWS Management Console

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.

- Разрешения:

  - **ReadOnlyAccess** - если вы планируете только запускать опрос облачных сегментов и не планируете устанавливать приложения на инстансы EC2 с помощью AWS API;

  - **ReadOnlyAccess** и **AmazonSSMFullAccess** – если вы планируете и запускать опрос облачных сегментов, и устанавливать приложения на инстансы EC2 с помощью AWS API. В этом случае вам нужно назначить защищаемым инстансам EC2 IAM-роль с правами AmazonEC2RoleforSSM.

  После добавления разрешений внимательно их просмотрите. 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.

При развертывании Kaspersky Security Center в облачном сегменте вам потребуется указать, что вы пользуетесь учетной записью IAM-пользователя, и предоставить Kaspersky Security Center идентификатор ключа доступа и секретный ключ доступа.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky Security Center.

Создание IAM-роли для установки приложений на инстансы Amazon EC2

Прежде чем разворачивать защиту на инстансах EC2 средствами Kaspersky Security Center, создайте в Консоли управления AWS IAM-роль с необходимыми правами для установки приложений на инстансы. Дополнительную информацию см. в разделах справки AWS, описывающих IAM-роли.

IAM-роль необходима для того, чтобы назначать ее на все инстансы EC2, на которые вы планируете устанавливать приложения безопасности с помощью Kaspersky Security Center. Если вы не назначите инстансу IAM-роль, обладающую необходимыми правами, установка приложений средствами AWS API на этот инстанс завершится с ошибкой.

Для работы с Консолью управления AWS вам понадобятся имя пользователя и пароль от учетной записи в AWS.

Чтобы создать IAM-роль для установки приложений на инстансы:

1. Откройте Консоль управления AWS и выполните вход под своей учетной записью AWS.

2. В меню слева выберите пункт **Roles**.

3. Нажмите на кнопку **Create Role**.

4. В отобразившемся списке сервисов выберите **EC2** и затем в списке **Select Your Use case** еще раз **EC2**.

5. Нажмите на кнопку **Далее: Права**.

6. В отобразившемся списке установите флажок напротив пункта **AmazonEC2RoleforSSM**.

7. Нажмите на кнопку **Далее: Просмотр**.

8. Введите имя и описание IAM-роли и нажмите на кнопку **Create role**.

   Созданная роль отобразится в списке ролей с именем и описанием, которые вы ввели.

В дальнейшем вы можете использовать созданную IAM-роль при создании новых инстансов EC2, которые вы будете защищать с помощью Kaspersky Security Center, а также ассоциировать ее с уже существующими инстансами.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky Security Center.

Работа с Amazon RDS

В этом разделе описывается, какие действия необходимо выполнить, чтобы подготовить базу данных Amazon Relational Database Service (RDS) для Kaspersky Security Center, поместить ее в группу параметров, создать IAM-роль для работы с базой RDS, подготовить корзину S3 для хранения данных и перенести базу данных в существующую базу RDS.

Amazon Relational Database Service (Amazon RDS) это веб-сервис, который помогает пользователям AWS настраивать, управлять и масштабировать реляционную базу данных в облачном окружении AWS. Вы можете использовать базу данных Amazon RDS для работы с Kaspersky Security Center.

Вы можете работать со следующими базами данных:

- Microsoft SQL Server
- SQL Express Edition
- Aurora MySQL 5.7
- Standard MySQL 5.7

Создание инстанса Amazon RDS

Если вы хотите использовать Amazon RDS в качестве СУБД, вы можете создать инстанс базы данных Amazon RDS. В этом разделе описано, как выбрать SQL Express Edition; если вы хотите работать с Aurora MySQL или Standard MySQL (версии 5.7, 8.0), вам нужно выбрать одно из этих ядер.

Чтобы создать инстанс базы данных Amazon RDS:

1. Откройте консоль управления AWS https://console.aws.amazon.com и войдите под своей учетной записью.

2. Используя интерфейс AWS, создайте базу данных со следующими параметрами:

   - Ядро: Microsoft SQL Server, SQL Express Edition.
   - Версия ядра базы данных: SQL Server 2014 12.00.5546.0v1.
   - Класс экземпляра базы данных: db.t2.medium.

- Тип хранилища: General purpose.
- Размер хранилища: минимум 50 ГиБ.
- Группа безопасности: та же группа, в которую входит инстанс EC2 с установленным Сервером администрирования Kaspersky Security Center.

Создайте идентификатор, имя пользователя и пароль для экземпляра RDS.

Вы можете оставить значения всех параметров по умолчанию. Или измените значения параметров, заданных по умолчанию, если вы хотите настроить инстанс Amazon RDS. Подробную информацию смотрите на справочных страницах AWS.

3. На последнем шаге AWS отображает результат процесса. Если вы хотите просмотреть подробную информацию инстанса Amazon RDS, нажмите на **View DB instance details**. Если вы хотите перейти к следующему действию, создайте группы параметров для инстанса Amazon RDS.

Создание инстанса Amazon RDS занимает несколько минут. После того как инстанс создан, вы можете использовать его для работы с данными Kaspersky Security Center.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky Security Center.

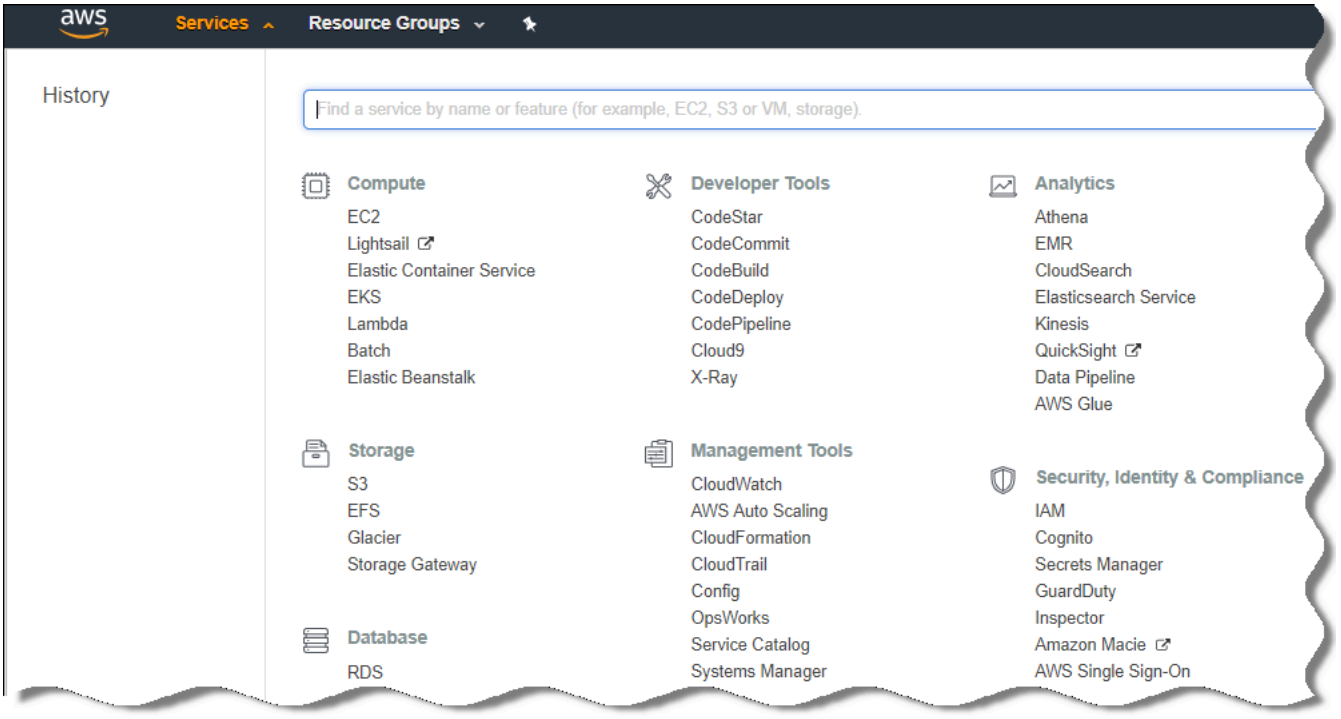
Создание группы параметров для инстанса Amazon RDS

Вам нужно поместить инстанс Amazon RDS в группу параметров.

Чтобы создать группу параметров для инстанса Amazon RDS:

1. Убедитесь, что Консоль управления AWS (https://console.aws.amazon.com) открыта и вы вошли под вашей учетной записью.
2. В меню выберите пункт **Службы**.

   Отобразится список доступных служб (см. рис. ниже).



Список сервисов в AWS Management Console

3. В списке выберите **RDS**.

4. В левой панели нажмите на **Option groups**.

5. Нажмите на кнопку **Create group**.

6. Создайте группу параметров со следующими параметрами (если вы выбрали SQL Server на шаге создания инстанса Amazon RDS):

   - Ядро: SQLserver-ex.
   - Основная версия ядра: 12.00.

   Если вы выбрали базу данных, отличную от SQL, на этапе создания инстанса Amazon RDS, выберите соответствующее ядро.

Группа создана и отображается в списке групп.

После создания группы параметров поместите инстанс Amazon RDS в эту группу параметров.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky Security Center.

Изменение группы параметров

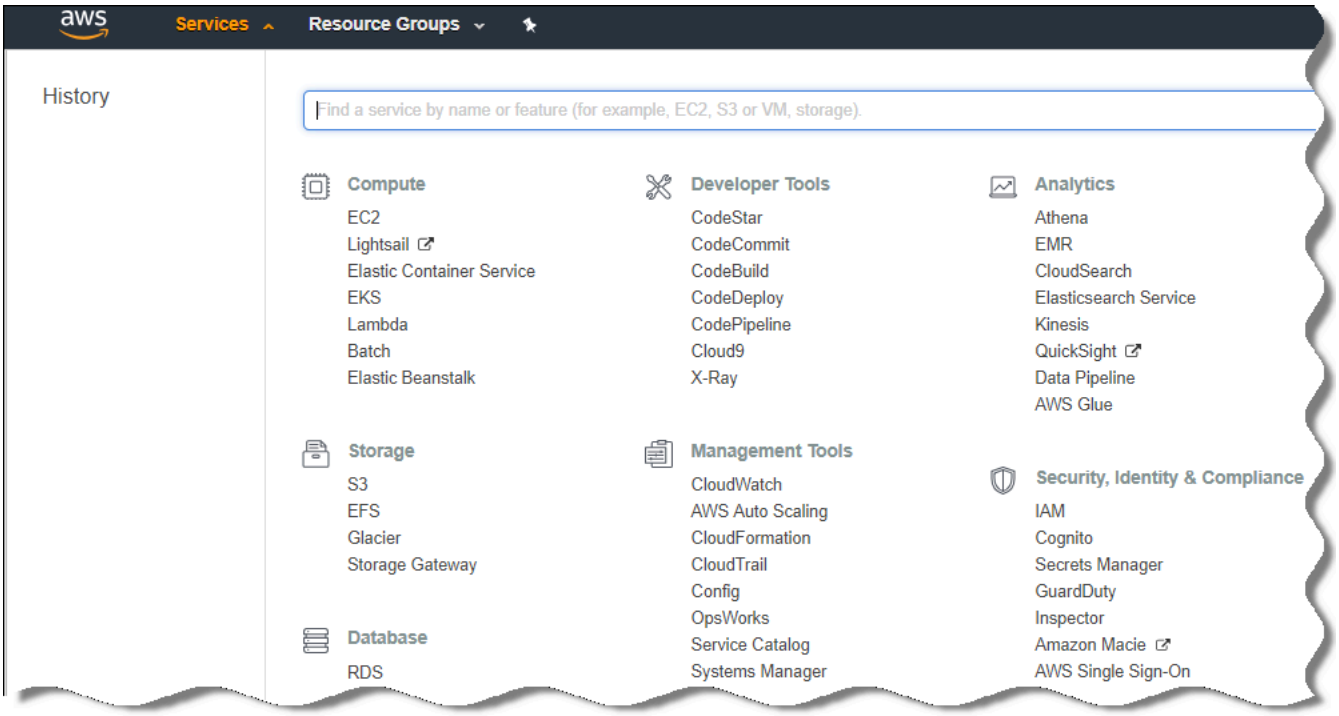
Заданная по умолчанию конфигурация группы параметров, в которую вы поместили инстанс Amazon RDS, не достаточна для работы с базой данных Kaspersky Security Center. Необходимо добавить параметры в группу параметров и создать IAM-роль для работы с базой данных.

Чтобы изменить группу параметров и создать IAM-роль:

1. Убедитесь, что Консоль управления AWS (https://console.aws.amazon.com) открыта и вы вошли под вашей учетной записью

2. В меню выберите пункт **Службы**.

   Отобразится список доступных служб (см. рис. ниже).



Список сервисов в AWS Management Console

3. В списке выберите RDS.

4. В левой панели нажмите на **Option groups**.

   Отобразится список групп параметров.

5. Выберите группу параметров, в которую вы поместили инстанс Amazon RDS, и нажмите на кнопку **Добавить параметр**.

   Откроется окно **Добавить параметр**.

6. В разделе IAM-роль выберите параметр **Create a new role** / **Yes** и введите имя новой IAM-роли.

   Роль создана с набором прав по умолчанию. Позже вы можете изменить эти права.

7. В разделе корзины S3 выполните одно из следующих действий:

   - Если инстанс корзины Amazon S3 для резервной копии не создан, перейдите по ссылке **Создать корзину S3** и создайте корзину S3, используя интерфейс AWS.

   - Если вы уже создали инстанс корзины Amazon S3 для резервной копии данных Сервера администрирования, выберите требуемую корзину S3 из раскрывающегося меню.

8. Чтобы завершить добавление параметров, нажмите на кнопку **Добавить параметр** в нижней части страницы.

Вы изменили группу параметров и создали IAM-роль для работы с базы RDS.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky Security Center.

Изменение прав IAM-роли для инстанса базы данных Amazon RDS

После того, как вы добавили параметры в группу параметров, вам необходимо назначить требуемые права IAM-роли, созданной для работы с инстансом базы данных Amazon RDS.

Чтобы назначить требуемые права IAM-роли, которую вы создали для работы с инстансом базы данных Amazon RDS:

1. Убедитесь, что Консоль управления AWS (https://console.aws.amazon.com) открыта и вы вошли под вашей учетной записью
2. В списке служб выберите **IAM**.

   Откроется окно, содержащее список имен пользователей и меню, с помощью которого вы сможете работать с инструментом.
3. В меню выберите **Роли**.
4. В списке IAM-ролей выберите роль, которую вы создали во время добавления параметров в группу параметров.
5. Используя интерфейс AWS, удалите политику **sqlNativeBackup-<date>**.
6. Используя интерфейс AWS назначьте политику **AmazonS3FullAccess** роли.

IAM-роль получает требуемые права для работы с Amazon RDS.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky Security Center.

Подготовка корзины Amazon S3 для базы данных

Если вы планируете использовать базу данных Amazon Relational Database System (Amazon RDS), вам потребуется создать инстанс корзины Buzz Amazon Simple Storage Service (Amazon S3), в котором будет храниться обычная резервная копия данных. Подробную информацию об Amazon S3 и корзинах S3 см. в справке Amazon. Подробную информацию о создании инстанса Amazon S3 см. в справке Amazon S3.

Чтобы создать корзину Amazon S3:

1. Убедитесь, что Консоль управления AWS открыта и вы вошли под вашей учетной записью.
2. В списке служб AWS выберите S3.
3. Перейдите в консоль, чтобы создать корзину, и следуйте далее указаниям мастера.

4. Выберите такой же регион, в котором расположен ваш Сервер администрирования (или будет расположен).

5. На последнем шаге убедитесь, что новая корзина появилась в списке корзин.

   Корзина S3 создана и отображается в списке корзин. Вы можете указать корзину при добавлении параметра в группу параметров. Вы можете также указать адрес вашей корзины S3 в Kaspersky Security Center при создании задачи *Резервное копирование данных Сервера администрирования* в Kaspersky Security Center.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky Security Center.

Перенос базы данных в Amazon RDS

Вы можете перенести вашу базу данных Kaspersky Security Center с локального устройства на инстанс Amazon S3, который поддерживает Amazon RDS. Для этого вам необходимы корзина S3 для базы RDS и учетная запись IAM-пользователя с правами AmazonS3FullAccess для этой корзины S3.

Чтобы перенести базу данных:

1. Убедитесь, что вы создали инстанс RDS (подробную информацию см. на справочных страницах Amazon RDS).

2. На вашем физическом Сервере администрирования (локальном), запустите утилиту резервного копирования "Лаборатории Касперского" для данных Сервера администрирования.

   Убедитесь, что файл называется backup.zip.

3. Скопируйте файл backup.zip на инстанс EC2, на котором установлен Сервер администрирования.

   Убедитесь, что на инстансе EC2, на котором установлен Сервер администрирования, достаточно свободного дискового пространства. В окружении AWS вы можете добавить дисковое пространство для вашего инстанса, чтобы выполнить процесс переноса базы данных.

4. Снова запустите утилиту резервного копирования "Лаборатории Касперского" в неинтерактивном режиме на Сервере администрирования в AWS.

   В результате запустится мастер выполнения резервного копирования и восстановления данных.

5. На шаге **Выберите действие** выберите пункт **Выполнить восстановление данных Сервера администрирования** и нажмите на кнопку **Далее**.

6. На шаге **Параметры восстановления** нажмите на кнопку **Обзор** рядом с полем **Папка для хранения резервных копий**.

7. В открывшемся окне **Войти в онлайн-хранилище** заполните следующие поля и нажмите на кнопку **ОК**:

   - **Имя корзины S3**

     Имя корзины Amazon S3.

   - **Папка резервных копий данных**

     Укажите расположение папки, предназначенной для хранения резервных копий.

- **ID ключа доступа**

  Ключ доступа AWS IAM, принадлежащий IAM-пользователю с правами использования корзины Amazon S3 (права AmazonS3FullAccess).

- **Секретный ключ**

  Секретный ключ AWS IAM, принадлежащий IAM-пользователю с правами использования корзины Amazon S3 (права AmazonS3FullAccess).

8. Выберите параметр **Перенести из локальной резервной копии данных**. Станет доступна кнопка **Обзор**.

9. Нажмите на кнопку **Обзор** и выберите на Сервере администрирования AWS папку, в которую вы поместили файл backup.zip.

10. Нажмите на кнопку **Далее** и завершите процедуру.

Данные будут храниться в базе RDS с использованием корзины S3. Вы можете использовать эту базу данных для дальнейшей работы с Kaspersky Security Center в окружении AWS.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky Security Center.

Работа в облачном окружении Microsoft Azure

В этом разделе представлена информация о том, как развернуть и поддерживать Kaspersky Security Center в облачном окружении, предоставленном платформой Microsoft Azure, и как развернуть защиту на виртуальных машинах внутри облачного окружения.

В Kaspersky Security Center, который был развернут с использованием подписки с ежемесячной тарификацией в зависимости от объема услуг, возможности Системного администрирования активируются автоматически, но Управление мобильными устройствами не может быть активировано.

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 развертыванием Сервера администрирования создайте ID приложения в Azure с правами, необходимыми для установки приложений на виртуальные машины.

Если вы приобрели образ Kaspersky Security Center в магазине Azure Marketplace, вы можете развернуть виртуальную машину с готовым образом AMI Сервера администрирования Kaspersky Security Center. Вам нужно выбрать параметры виртуальной машины, но вам не нужно устанавливать приложения самостоятельно. После установки вы можете запустить Консоль администрирования и подключиться к Серверу администрирования, чтобы начать работу с Kaspersky Security Center.

Вы также можете использовать виртуальную машину Azure с развернутым на нем Сервером администрирования Kaspersky Security Center для защиты физических устройств (например, если такой облачный сервер оказывается выгоднее в обслуживании и содержании, чем физический). В этом случае работа с Сервером администрирования будет устроена так же, как если бы Сервер администрирования был установлен на физическом устройстве. Если вы не планируете использовать инструменты Azure API, ID приложения в Azure вам не нужен. В этом случае подписки Azure достаточно.

Создание подписки, идентификатора приложения и пароля

Для работы с Kaspersky Security Center 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 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.

   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.

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 на виртуальных машинах, вашему ID приложения в Azure должна быть назначена роль Участник виртуальных машин (Virtual Machine Contributor).

Следуйте инструкциям, приведенным на веб-сайте Microsoft, чтобы назначить роль для ID приложения в Azure.

Развертывание Сервера администрирования в Microsoft Azure и выбор базы данных

Чтобы развернуть Сервер администрирования в окружении Microsoft Azure:

1. Войдите в Microsoft Azure, используя свою учетную запись.
2. Перейдите на портал Azure.
3. В левой части панели нажмите на зеленый значок плюса.
4. Напишите "Kaspersky Security для виртуальных и облачных сред" в поле поиска меню.

   Kaspersky Security для виртуальных и облачных сред – это комбинация Kaspersky Security Center и двух приложений безопасности для защиты инстансов: Kaspersky Endpoint Security для Linux и Kaspersky Security для Windows Server.
5. В списке результатов выберите Kaspersky Security для виртуальных и облачных сред или Kaspersky Security для виртуальных и облачных сред (BYOL).

   В правой части экрана отобразится информационное окно.
6. Прочитайте информацию и нажмите на кнопку Создать в информационном окне.
7. Заполните требуемые поля. Используйте подсказки и справку, чтобы получить информацию и помощь.
8. При выборе размера выберите один из трех параметров.

   В большинстве случаев 8 ГБ оперативной памяти достаточно. Однако в Azure вы можете увеличить размер оперативной памяти и других ресурсов виртуальной машины в любое время.
9. При выборе базы данных выберите один из следующих вариантов, в соответствии с вашим планом:

   - Локальная. Если вам нужна база данных на той же виртуальной машине, на которой будет развернут Сервер администрирования. Kaspersky Security Center поставляется с базой данных SQL Server Express. Выберите этот параметр, если базы данных SQL Server Express достаточно для ваших потребностей.
   - Новая. Если вы хотите создать новую базу RDS в окружении Azure, выберите этот параметр, если вы хотите использовать СУБД, отличную от SQL Server Express. Ваши данные будут перенесены в облачное окружение, где они останутся, и у вас не будет никаких дополнительных затрат.
   - Существующая. Если вы хотите использовать существующий сервер базы данных. В этом случае вам нужно указать его месторасположение. Если сервер вне окружения Azure, ваши данные будут перенесены через интернет, что может привести к дополнительным расходам.
10. При вводе идентификатора подписки используйте подписку, созданную ранее.

После развертывания вы можете подключиться к Серверу администрирования с помощью RDP. Вы можете использовать Консоль администрирования для работы с Сервером администрирования.

Работа с Azure SQL

В этом разделе описаны действия, необходимые для подготовки базы данных Microsoft Azure к использованию Kaspersky Security Center, а также для подготовки учетной записи хранения Azure и переноса существующей базы данных в Azure SQL.

База данных SQL это универсальная служба управления реляционными базами данных в Microsoft Azure.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky Security Center.

Создание учетной записи хранения Azure

В Microsoft Azure требуется создать учетную запись хранения для работы с базой данных Azure SQL и для скриптов развертывания.

Чтобы создать учетную запись хранения:

1. Выполните вход на портал Azure.
2. В левой панели выберите пункт **Учетные записи хранения** и перейдите в окно **Учетные записи хранения**.
3. В окне **Учетные записи хранения** нажмите на кнопку **Добавить**, чтобы перейти в окно **Создание учетной записи хранения**.
4. Заполните все необходимые поля для создания учетной записи хранения:
   - Местоположение: должно совпадать с местоположением (географическим регионом) Сервера администрирования.
   - Прочие поля: можно оставить указанные по умолчанию значения.

   Используйте подсказки, чтобы получить информацию о каждом поле.

   После создания учетной записи хранения отобразится список ваших учетных записей хранения.
5. В списке учетных записей хранения выделите созданную учетную запись, чтобы посмотреть информацию о ней.
6. Убедитесь, что вам известны имя учетной записи, группа ресурсов и ключи доступа для этой учетной записи хранения. Эти данные понадобятся вам при работе с Kaspersky Security Center.

Справку можно посмотреть на веб-сайте Azure.

Если у вас уже есть учетная запись хранения, ее можно использовать для работы с Kaspersky Security Center.

Создание базы данных Azure SQL и SQL-сервера

В окружении Azure вам понадобится база данных SQL и SQL-сервер.

Чтобы создать базу данных Azure SQL и SQL-сервер:

1. Выполните инструкции, приведенные на веб-сайте Azure.

   Вы можете создать новый сервер, когда появится приглашение от Microsoft Azure. Если у вас уже есть Azure SQL Server, вы можете использовать его для Kaspersky Security Center, а не создавать новый сервер.

2. После создания базы данных SQL и SQL-сервера убедитесь, что вам известны имя ресурса и группа ресурсов.

   a. Перейдите по ссылке https://portal.azure.com и убедитесь, что выполнен вход.

   b. На левой панели выберите пункт **Базы данных SQL**.

   c. Выберите имя базы данных в списке баз данных.

      Откроется окно свойств.

   d. Имя базы данных является именем ресурса. Имя группы ресурсов отображается в окне свойств в разделе **Обзор**.

Имя ресурса и группа ресурсов базы данных понадобятся вам при переносе базы данных в Azure SQL.

Перенос базы данных в Azure SQL

После развертывания Сервера администрирования в окружении Microsoft Azure можно выполнить перенос базы данных Kaspersky Security Center с физического устройства в Azure SQL. Для использования базы данных Azure SQL необходима учетная запись хранения Azure. Также у вас должен быть Microsoft SQL Server и Платформа приложения уровня данных (DacFx) и SQLSysCLRTypes на вашем Сервере администрирования.

Чтобы перенести базу данных:

1. Убедитесь, что вы создали учетную запись хранения Azure.

2. Убедитесь, что на Сервере администрирования есть SQLSysCLRTypes и DacFx.

   Вы можете загрузить Microsoft SQL Server Data-Tier Application Framework (17.0.1 DacFx) и SQLSysCLRTypes (выберите версию, соответствующую версии вашего SQL Server) с официального сайта Microsoft.

3. На вашем физическом Сервере администрирования запустите утилиту резервного копирования "Лаборатории Касперского" для данных Сервера администрирования с включенным параметром **Перенести в формат Azure**.

4. Поместите файл резервной копии данных на Сервер администрирования в Azure.

   > Убедитесь, что на виртуальной машине Azure, на которой установлен Сервер администрирования, достаточно свободного дискового пространства. В окружении Azure можно добавить дисковое пространство для виртуальной машины, чтобы обеспечить процесс переноса базы данных.

5. На Сервере администрирования, расположенного в облачном окружении Microsoft Azure, еще раз запустите утилиту резервного копирования "Лаборатории Касперского" в интерактивном режиме.

   В результате запустится мастер выполнения резервного копирования и восстановления данных.

6. На шаге **Выберите действие** выберите пункт **Выполнить восстановление данных Сервера администрирования** и нажмите на кнопку **Далее**.

7. На шаге **Параметры восстановления** нажмите на кнопку **Обзор** рядом с полем **Папка для хранения резервных копий**.

8. В открывшемся окне **Войти в онлайн-хранилище** заполните следующие поля и нажмите на кнопку **ОК**:

   - **Имя учетной записи хранения Azure**

     Вы создали имя учетной записи хранения Azure для работы с Kaspersky Security Center.

   - **Папка резервных копий данных**

     Укажите расположение папки, предназначенной для хранения резервных копий.

   - **Идентификатор подписки Azure**

     Вы создали подписку на портале Azure.

   - **Пароль приложения в 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.

   - **Ключ доступа хранилища Azure**

     Доступен в свойствах учетной записи хранения в разделе "Access Keys". Вы можете использовать любой ключ (key1 или key2).

   - **Имя SQL-сервера Azure**

     Доступно в свойствах SQL-сервера Azure.

   - **Группа источника SQL-сервера Azure**

     Доступно в свойствах SQL-сервера Azure.

   - **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.

9. Выберите параметр **Перенести из локальной резервной копии данных**.

   Станет доступна кнопка **Обзор**.

10. Нажмите на кнопку **Обзор** и выберите на Сервере администрирования в Azure папку, в которую вы поместили файл резервной копии данных.

11. Нажмите на кнопку **Далее** и завершите процедуру.

Данные будут восстановлены в базу данных Azure SQL с использованием хранилища Azure. Вы можете использовать эту базу данных для дальнейшей работы с Kaspersky Security Center в окружении Azure.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky Security Center.

Работа в Google Cloud

Этот раздел содержит информацию о работе с Kaspersky Security Center в облачном окружении, предоставляемом Google.

Создание электронной почты клиента, идентификатора проекта и закрытого ключа

API Google можно использовать для работы с Kaspersky Security Center 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 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.

Работа с экземпляром Google Cloud SQL для MySQL

Вы можете создать базу данных в Google Cloud и использовать эту базу данных для Kaspersky Security Center.

Kaspersky Security Center работает с MySQL 5.7 и 5.6. Другие версии MySQL не тестировались.

Чтобы создать и настроить базу данных MySQL:

Откройте в браузере страницу https://cloud.google.com/sql/docs/mysql/create-instance#create-2nd-gen и следуйте инструкциям.

При настройке базы данных MySQL используйте следующие флаги:

- **sort_buffer_size** 10000000;
- **join_buffer_size** 20000000;
- **innodb_lock_wait_timeout** 300;
- **max_allowed_packet** 32000000;
- **innodb_thread_concurrency** 20;
- **max_connections** 151;
- **tmp_table_size** 67108864;
- **max_heap_table_size** 67108864;
- **lower_case_table_names** 1.

Подготовка клиентских устройств в облачном окружении для работы с Kaspersky Security Center

Устройства, на которые вы планируете установить Сервер администрирования, Агент администрирования и приложения безопасности "Лаборатории Касперского", должны соответствовать следующим условиям:

- Настройки групп безопасности делают доступными следующие порты на Сервере администрирования (минимально необходимый для развертывания набор портов):
  - 8060 HTTP – для передачи с Сервера администрирования на защищаемые инстансы инсталляционных пакетов Агента администрирования и приложений безопасности;
  - 8061 HTTP – для передачи с Сервера администрирования на защищаемые инстансы инсталляционных пакетов Агента администрирования и приложений безопасности;
  - 13000 TCP – для передачи с защищаемых инстансов и подчиненных Серверов администрирования на главный Сервер администрирования с помощью SSL;
  - 13000 UDP – для передачи на Сервер администрирования информации о выключении инстансов;
  - 14000 TCP – для передачи с защищаемых инстансов и подчиненных Серверов администрирования на главный Сервер администрирования без SSL;
  - 13291 – для подключения Консоли администрирования к Серверу администрирования;
  - 40080 – для работы скриптов развертывания.

  Вы можете настроить группы безопасности в Консоли управления AWS или на портале Azure. Если вы планируете использовать Kaspersky Security Center в конфигурации, отличной от настроек по умолчанию, см. Базу знаний. Примеры конфигураций, отличных от конфигураций по умолчанию, не включают установку Консоли администрирования на устройстве с Сервером администрирования, но включают установку на вашу рабочую станцию или использование прокси-сервера KSN.

- На клиентских устройствах доступен порт 15000 UDP (для приема запросов на связь с Сервером администрирования).
- В облачном окружении AWS:
  - Если вы планируете использовать API AWS, задается IAM-роль, под которой будут устанавливаться приложения на инстансах.
  - На каждом инстансе Amazon EC2, Systems Manager Agent (SSM-агент) установлен и запущен.
  - SSM-агент позволяет Kaspersky Security Center автоматически устанавливать приложения на устройства и группы устройств, не запрашивая каждый раз подтверждение от администратора.
  - На инстансах под управлением операционной системы Windows, развернутых из образов AMI позже ноября 2016 года, SSM-агент установлен и работает. На все остальные устройства вам потребуется устанавливать SSM-агент самостоятельно. Подробнее об установке SSM-агента на устройства под управлением операционных систем Windows и Linux см. на странице справки AWS.
- В облачном окружении Microsoft Azure:
  - На каждой виртуальной машине Azure установлен и запущен Azure VM Agent.

    По умолчанию виртуальная машина создается с Azure VM Agent и вы не должны устанавливать или включать его вручную. Дополнительные сведения Azure VM Agent на устройствах Windows и на устройствах Linux см. страницах справки Microsoft.
  - Ваш ИД приложения в Azure имеет следующие роли:
    - Читатель (обнаруживает виртуальные машины при опросе сети).
    - Участник виртуальной машины (разворачивает защиту на виртуальных машинах).
    - SQL Server Contributor (использует базу данных SQL в облачном окружении Microsoft Azure).

    Если вы хотите выполнять все эти операции, назначьте все три роли вашему идентификатору приложения в Azure.

Создание инсталляционных пакетов, необходимых для настройки облачного окружения

Мастер настройки облачного окружения в Kaspersky Security Center доступен при наличии инсталляционных пакетов и плагинов управления следующих приложений:

- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Windows

  Развертывание Kaspersky Endpoint Security для Windows в облачном окружении будет доступно после выхода версии Kaspersky Endpoint Security 12.0 для Windows.
- Kaspersky Security для Windows Server

Эти инсталляционные пакеты требуются для установки приложений на инстансах и виртуальных машинах, которые вы хотите защитить. Если у вас нет этих инсталляционных пакетов, вам нужно их создать. Иначе мастер настройки облачного окружения не будет запущен.

Для создания инсталляционных пакетов:

1. Загрузите последние версии приложений и плагинов с сайта "Лаборатории Касперского":
   - Установщик и плагин управления Kaspersky Security для Windows Server.
   - Установщик, файлы для удаленной установки с помощью Kaspersky Security Center и плагин управления Kaspersky Endpoint Security для Linux.
2. Сохраните все файлы на инстансе (или виртуальной машине), где установлен Сервер администрирования.
3. Извлеките файлы из всех пакетов.
4. Запустите Kaspersky Security Center.
5. В дереве консоли перейдите в раздел **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты** и нажмите на кнопку **Создать инсталляционный пакет**.
6. Выберите **Создать инсталляционный пакет "Лаборатории Касперского"**.
7. Укажите название пакета и путь к установщику приложения: <folder>\<file name>.kud и нажмите на кнопку **Далее**.
8. Прочтите Лицензионное соглашение, установите флажок, подтверждающий, что вы принимаете его условия и нажмите на кнопку **Далее**.

Инсталляционный пакет загружен на Сервер администрирования и доступен в списке инсталляционных пакетов.

Настройка облачного окружения станет доступна, как только вы создадите инсталляционные пакеты и установите плагины управления на Сервер администрирования.

Настройка облачного окружения

Чтобы настроить Kaspersky Security Center с использованием мастера настройки облачного окружения, вам потребуется следующее:

- Укажите учетные данные для облачного окружения:
  - IAM-роль, которой было предоставлено право опроса облачного сегмента, или учетная запись IAM-пользователя, которому было 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.

Если вы не хотите использовать возможности работы в облачном окружении (например, в случае, если вы хотите управлять защитой только физических клиентских устройств), вы можете выйти из мастера настройки облачного окружения и вручную запустить стандартный мастер первоначальной настройки Сервера администрирования.

Настройка облачного окружения запускается автоматически при первом подключении к Серверу администрирования через Консоль администрирования, если вы разворачиваете Kaspersky Security Center из готового образа AMI. Вы также можете запустить мастер настройки облачного окружения в любое время.

Чтобы запустить мастер настройки облачного окружения вручную:

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню узла выберите пункт **Все задачи → Настройка работы в облачном окружении**.

Приблизительное время настройки составляет около 15 минут.

О мастере настройки облачного окружения

Мастер настройки облачного окружения позволяет настроить Kaspersky Security Center с учетом особенностей работы в облачном окружении.

В результате работы мастера будут созданы следующие объекты:

- политику Агента администрирования с настройками по умолчанию;
- политику Kaspersky Endpoint Security для Linux;
- политику Kaspersky Security для Windows Server;
- группу администрирования и правило автоматического перемещения инстансов в эту группу администрирования;
- задачу резервного копирования данных Сервера администрирования;
- задачи установки защиты на устройства под управлением Linux и Windows;

- задачи для каждого из управляемых устройств:
  - быстрый поиск вредоносного ПО;
  - загрузку обновлений.

Если вы выбрали вариант лицензирования по модели BYOL, то настройка облачного окружения также активирует Kaspersky Security Center с помощью файла ключа или кода активации и помещает файл ключа или код активации в хранилище лицензий.

Шаг 1. Выбор способа активации приложения

Этот шаг не отображается, если вы подписывались на один из готовых образов AMI (в магазине приложений AWS Marketplace) или используете ежемесячный счет за использование SKU (в магазине Azure Marketplace). В этом случае мастер сразу отобразит следующий шаг. Вы не можете приобрести готовый образ AMI для Google Cloud.

Если вы выбрали вариант лицензирования по схеме BYOL для Kaspersky Security Center, мастер предложит вам выбрать способ активации приложения.

Активируйте приложение с помощью кода активации (или файла ключа) для приложения Kaspersky Security для виртуальных сред или приложения Kaspersky Security для виртуальных и облачных сред.

Вы можете активировать приложение следующими способами:

- Ввести код активации.

  Запустится процесс онлайн-активации. В ходе этого процесса выполняется проверка указанного кода активации, получение и активация файла ключа.

- Указать файл ключа.

  Приложение проверит файл ключа и либо активирует его, если в нем содержится корректная информация, либо предложит указать другой файл ключа.

Kaspersky Security Center помещает лицензионный ключ в хранилище лицензий и помечает его как автоматически распространяемый на управляемые устройства.

Если вы подключаетесь к инстансу с помощью стандартного приложения Microsoft Windows "Подключение к удаленному рабочему столу" (Remote Desktop Connection) или аналогичным приложением, требуется указать в свойствах удаленного подключения диск физического устройства, с которого вы подключаетесь. Таким образом вы обеспечите доступ с инстанса к файлам на вашем физическом устройстве и сможете выбрать и указать файл ключа.

При работе с Kaspersky Security Center, развернутым из платного образа AMI, или при использовании SKU с ежемесячным выставлением счетов за использование, в хранилище лицензий невозможно добавлять файлы ключей или коды активации.

Шаг 2. Выбор облачного окружения

Выберите облачное окружение, в котором вы разворачиваете Kaspersky Security Center: AWS, Azure или Google Cloud.

Шаг 3. Аутентификация в облачном окружении

AWS

Если вы выбрали AWS, либо укажите, что у вас есть IAM-роль с необходимыми правами, либо предоставьте Kaspersky Security Center ключ доступа AWS IAM. Без IAM-роли или ключа доступа AWS IAM невозможен опрос облачных сегментов.

Укажите следующие параметры соединения, которое в дальнейшем будет использоваться для опроса облачного сегмента:

- **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".

- **Использовать AWS IAM-роль**

  Выберите этот вариант, если вы уже создали IAM-роль для работы Сервера администрирования с сервисами AWS.

- **Использовать учетную запись AWS IAM-пользователя**

  Выберите этот вариант, если у вас есть учетная запись IAM-пользователя с необходимыми правами и вы можете ввести ID ключа и секретный ключ.

  - **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, а не IAM-роль.

  - **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, а не IAM-роль.

Соединение будет сохранено в параметрах приложения. С помощью настройки облачного окружения вы можете создать только один ключ доступа AWS IAM. Впоследствии вы можете указывать и другие соединения для управления другими облачными сегментами.

Если вы хотите устанавливать приложения на инстансы средствами Kaspersky Security Center, необходимо, чтобы ваша IAM-роль (либо IAM-пользователь, учетной записи которого соответствует вводимый вами ключ), имела необходимые привилегии.

Azure

Если вы выбрали Azure, укажите следующие параметры соединения, которые в дальнейшем будут использоваться для опроса облачного сегмента:

- **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".

- **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 в 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.

- **Имя учетной записи хранения Azure**

  Вы создали имя учетной записи хранения Azure для работы с Kaspersky Security Center.

- **Ключ доступа хранилища Azure**

  Вы получили пароль (ключ) при создании учетной записи хранения Azure для работы с Kaspersky Security Center.

  Ключ доступен в разделе "Overview of the Azure storage account" в подразделе "Keys".

Соединение будет сохранено в параметрах приложения.

Google Cloud

Если вы выбрали Google Cloud, укажите следующие параметры соединения, которые в дальнейшем будут использоваться для опроса облачного сегмента:

- **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".

- **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.

Соединение будет сохранено в параметрах приложения.

Шаг 4. Настройка синхронизации с облачным окружением и определение дальнейших действий

На этом шаге начинается опрос облачного сегмента и создается специальная группа администрирования для инстансов. Инстансы, обнаруженные при опросе, перемещаются в эту группу. Настраивается расписание опроса облачного сегмента (по умолчанию каждые 5 минут).

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**.

На странице **Синхронизация с облачным сегментом** можно задать следующие параметры:

- **Синхронизировать группы администрирования со структурой облачного сегмента**

  Если флажок установлен, то внутри группы **Управляемые устройства** автоматически создается группа **AWS** и запускается сканирование облачной сети. Виртуальные машины, обнаруженные во время каждого сканирования облачной сети, перемещаются в группу AWS. Структура подгрупп администрирования внутри группы AWS соответствует структуре вашего облачного сегмента. Устройства, не идентифицированные как инстансы Amazon EC2, находятся в группе **Нераспределенные устройства**. Такая структура групп позволяет устанавливать антивирусные программы на инстансы с помощью задач групповой установки и настраивать разные политики для разных групп.

Если флажок не установлен, то группа AWS также создается и опрос сети также запускается, однако внутри группы не создаются подгруппы, соответствующие структуре облачного сегмента. Все найденные инстансы находятся в группе администрирования AWS и отображаются единым списком. Если в процессе работы с Kaspersky Security Center вам потребуется произвести синхронизацию, то вы сможете изменить свойства правила **Синхронизация с AWS** и форсировать его. Форсирование правила перестраивает структуру групп внутри группы AWS так, чтобы она соответствовала структуре вашего облачного сегмента.

По умолчанию флажок снят.

- **Развернуть защиту**

  Если этот флажок установлен, то мастер создает задачу установки защитных программ на инстансы. После завершения работы мастера автоматически запустится мастер развертывания защиты на инстансы EC2 в ваших облачных сегментах, и вы сможете установить на них Агент администрирования и программы защиты.

  Если у IAM-пользователя, от имени которого работает Kaspersky Security Center, или у IAM-роли, которую вы используете, нет прав на установку программ на инстансы, то рекомендуется разворачивать защиту с помощью скриптов развертывания.

  Если флажок снят, то мастер развертывания защиты не запускается и задачи установки защитных программ на инстансы не создаются. Вы можете произвести оба эти действия позже вручную.

  По умолчанию флажок установлен.

Вы можете выполнить развертывание Google Cloud только с помощью инструментов Kaspersky Security Center. Если вы выбрали Google Cloud, вариант **Развернуть защиту** недоступен.

Шаг 5. Настройка Kaspersky Security Network в облачном окружении

Настройте параметры передачи информации о работе Kaspersky Security Center в базу знаний Kaspersky Security Network. Выберите один из следующих вариантов:

- **Я принимаю условия использования Kaspersky Security Network**

  Kaspersky Security Center и управляемые приложения, установленные на клиентских устройствах, в автоматическом режиме будут предоставлять информацию об их работе Kaspersky Security Network. Сотрудничество с Kaspersky Security Network обеспечивает более быстрое обновление баз данных о вирусах и угрозах, что увеличивает скорость реагирования на возникающие угрозы безопасности.

- **Я не принимаю условия использования Kaspersky Security Network**

  Kaspersky Security Center и управляемые приложения не будут предоставлять информацию о своей работе Kaspersky Security Network.

  Если вы выбрали этот параметр, использование Kaspersky Security Network будет выключено.

"Лаборатория Касперского" рекомендует участие в Kaspersky Security Network.

Шаг 6. Настройка параметров отправки уведомлений по электронной почте в облачном окружении

Настройте параметры рассылки оповещений о событиях, регистрируемых при работе приложений "Лаборатории Касперского" на виртуальных клиентских устройствах. Эти параметры будут использоваться в качестве значений по умолчанию в политиках приложений.

Для настройки рассылки оповещений о возникающих событиях приложений "Лаборатории Касперского" доступны следующие параметры:

- **Получатели (адреса электронной почты)**

  Адреса электронной почты пользователей, которым приложение будет отправлять уведомления. Вы можете указать один или более адресов. Если вы указываете несколько адресов, разделяйте их точкой с запятой.

- **SMTP-серверы**

  Адрес или адреса почтовых серверов вашей организации.

  Если вы указываете несколько адресов, разделяйте их точкой с запятой. Вы можете использовать следующие значения параметра:

  - IPv4-адрес или IPv6-адрес;
  - Имя устройства в сети Windows (NetBIOS-имя);
  - DNS-имя SMTP-сервера.

- **Порт SMTP-сервера**

  Номер коммуникационного порта SMTP-сервера. Если вы используете несколько SMTP-серверов, соединение с ними устанавливается через указанный коммуникационный порт. По умолчанию установлен порт 25.

- **Использовать ESMTP-аутентификацию**

  Включение поддержки ESMTP-аутентификации. После установки флажка можно указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию флажок снят.

Вы можете проверить установленные параметры отправки почтовых уведомлений с помощью кнопки **Отправить тестовое сообщение**. Если тестовое сообщение доставлено успешно по адресам, указанным в поле **Получатели (адреса электронной почты)**, то параметры настроены правильно.

Шаг 7. Создание первоначальной конфигурации защиты в облачном окружении

На этом шаге Kaspersky Security Center автоматически создает политики и задачи. В окне **Создание первоначальной конфигурации защиты** отображается список создаваемых приложением политик и задач.

Если вы используете базу RDS в облачном окружении AWS, вам необходимо предоставить ключ доступа IAM к Kaspersky Security Center при создании задачи резервного копирования Сервера администрирования. В этом случае заполните следующие поля:

- **Имя корзины S3**

  Имя корзины S3, которое вы создали для резервной копии данных.

- **ID ключа доступа**

  Вы получили ID ключа (последовательность из букв и цифр), когда создали учетную запись IAM-пользователя для работы с корзиной S3 в хранилище инстансов.

  Поле доступно, если вы выбрали базу RDS для контейнера S3.

- **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, а не IAM-роль.

Если вы используете базу данных Azure SQL в облачном окружении Azure, вам необходимо предоставить информацию о Azure SQL Server Kaspersky Security Center при создании задачи резервного копирования Сервера администрирования. В этом случае заполните следующие поля:

- **Имя учетной записи хранения Azure**

  Вы создали имя учетной записи хранения Azure для работы с Kaspersky Security Center.

- **Идентификатор подписки Azure**

  Вы создали подписку на портале Azure.

- **Пароль приложения в 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.

- **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.

- **Имя SQL-сервера Azure**

  Имя и группа источника доступны в свойствах SQL-сервера Azure.

- **Группа источника SQL-сервера Azure**

  Имя и группа источника доступны в свойствах SQL-сервера Azure.

- **Ключ доступа хранилища Azure**

  Доступен в свойствах учетной записи хранения в разделе "Access Keys". Вы можете использовать любой ключ (key1 или key2).

Если вы выполняете развертывание Сервера администрирования в Google Cloud, необходимо выбрать папку, в которой будут храниться резервные копии. Выберите папку на локальном устройстве или на экземпляре виртуальной машины.

Кнопка **Далее** станет доступна, когда все необходимые для минимальной конфигурации защиты политики и задачи будут созданы.

Если устройство, на котором должны выполняться задачи, не видимо в сети Сервера администрирования, задачи запускаются только тогда, когда устройство становится видимым. Если вы создаете EC2 или виртуальную машину Azure, может потребоваться некоторое время, прежде чем инстанс или виртуальная машина станут видимыми для Сервера администрирования. Если вы хотите, чтобы Агент администрирования и приложения безопасности были установлены на все новые устройства как можно скорее, убедитесь что параметр **Запускать пропущенные задачи** включен для задачи **Удаленная установка приложения**. В противном случае на созданные инстансы/виртуальные машины не будут уставлены Агент администрирования и приложения безопасности до тех пор, пока задача не запустится в соответствии с расписанием.

Шаг 8. Выбор действия, когда требуется перезагрузка операционной системы в ходе установки (для облачного окружения)

Если вы ранее выбрали **Развернуть защиту**, вам нужно выбрать действие, в случае если операционная система целевого устройства должна быть перезагружена. Если вы не выбрали параметр **Развернуть защиту**, это шаг пропускается.

Выберите, перезагружать ли инстансы, если в ходе установки приложений на устройства потребуется перезагрузка операционной системы:

- **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.

Если вы хотите принудительно закрыть все приложения в заблокированных сеансах на инстансах перед перезагрузкой, установите флажок **Принудительно закрывать приложения в заблокированных сеансах**. Если флажок не установлен, необходимо будет вручную закрыть все приложения, работающие на заблокированных инстансах.

Шаг 9. Получение обновлений Сервером администрирования

На этом шаге отображается прогресс загрузки обновлений, необходимых для корректной работы Сервера администрирования. Вы можете нажать на кнопку **Далее**, не дожидаясь окончания загрузки, чтобы перейти к завершающему окну мастера.

Мастер завершает работу.

Проверка успешности настройки

Чтобы проверить, правильно ли Kaspersky Security Center 15.1 настроен для работы в облачном окружении:

1. Запустите Kaspersky Security Center и убедитесь, что вы можете подключиться к Серверу администрирования через Консоль администрирования.
2. В дереве консоли выберите **Управляемые устройства****Cloud**.
3. Заходя в каждую подгруппу внутри группы **Управляемые устройства****Cloud**, убедитесь, что на вкладке **Устройства** отображаются все устройства каждой подгруппы.

   Если устройства не отображаются, вы можете выполнить опрос соответствующего облачного сегмента вручную, чтобы их найти.
4. Убедитесь, что на вкладке **Политики** имеются активные политики для приложений:

   - Агент администрирования Kaspersky Security Center.
   - Kaspersky Security для Windows Server
   - Kaspersky Endpoint Security для Linux

   Если политик нет в списке, вы можете создать их вручную.
5. Убедитесь, что на вкладке **Задачи** присутствуют задачи:

   - **Резервное копирование данных Сервера администрирования**
   - **Задача обновления для Windows Server**
   - **Обслуживание Сервера администрирования**
   - **Загрузка обновлений в хранилище Сервера администрирования**
   - **Поиск уязвимостей и требуемых обновлений**
   - **Установить защиту для Windows**
   - **Установить защиту для Linux**
   - **Задача быстрого опроса Windows Server**
   - **Быстрый опрос**
   - **Установить обновления для Linux**

   Если политик нет в списке, вы можете создать их вручную.

Kaspersky Security Center 15.1 корректно настроен для работы в облачном окружении.

Группа облачных устройств

Облачными устройствами можно управлять, объединяя их в группы. На этапе первоначальной настройки Kaspersky Security Center по умолчанию создает группу администрирования **Управляемые устройства\Cloud** и облачные устройства, обнаруженные во время опроса сети, перемещаются в эту группу.

Если вы установили флажок **Синхронизировать группы администрирования со структурой облачного сегмента** во время настройки синхронизации, то структура подгрупп в этой группе администрирования соответствует структуре ваших облачных сегментов. (Однако зоны доступности и группы размещения не представлены в структуре AWS, подсети не представлены в структуре Microsoft Azure.) Пустые подгруппы внутри группы, обнаруженные при опросе, автоматически удаляются.

Вы также можете самостоятельно создавать группы администрирования, объединяющие все или некоторые устройства.

Группа **Управляемые устройства\Cloud** по умолчанию наследует политики и задачи из группы **Управляемые устройства**. Вы можете изменить настройки параметров, если в свойствах параметров соответствующих политик и задач установлены флажки **Редактирование разрешено**.

Опрос облачного сегмента

Информацию о структуре сети и входящих в ее состав устройствах Сервер администрирования получает в ходе регулярных опросов облачных сегментов средствами AWS API, Azure API или Google API. На основании полученной информации Kaspersky Security Center 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 Сервер администрирования мог опрашивать облачные сегменты, необходимы права, которые обеспечивает IAM-роль или учетная запись IAM-пользователя (в AWS), идентификатор приложения и пароль (в Azure) или адрес электронной почты клиента Google, идентификатор проекта Google и закрытый ключ.

Вы можете добавлять и удалять соединения, а также настраивать для каждого облачного сегмента расписание опроса.

Добавление соединений для опроса облачных сегментов

Чтобы добавить соединение для опроса облачных сегментов в список доступных:

1. В дереве консоли выберите узел **Обнаружение устройств → Cloud**.
2. В рабочей области окна нажмите **Настроить параметры опроса**.

   Откроется окно свойств со списком соединений, используемых для опроса облачных сегментов.
3. Нажмите на кнопку **Добавить**.

   Отобразится окно **Соединение**.

4. Укажите имя облачного окружения для соединения, которое в дальнейшем будет использоваться для опроса облачного сегмента:

   Облачное окружение

   Облачное окружение, в котором расположены инстансы EC2 (или виртуальные машины), может быть Amazon Web Services (AWS), Microsoft Azure или Google Cloud.

   Если вы выбрали AWS, укажите следующие параметры:

   - **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".

   - **Использовать AWS IAM-роль**

     Выберите этот вариант, если вы уже создали IAM-роль для работы Сервера администрирования с сервисами AWS.

   - **Использовать учетную запись AWS IAM-пользователя**

     Выберите этот вариант, если у вас есть учетная запись IAM-пользователя с необходимыми правами и вы можете ввести ID ключа и секретный ключ.

     - **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, а не IAM-роль.

     - **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, а не IAM-роль.

   Мастер настройки облачного окружения дает возможность указать только один ключ доступа AWS IAM. Впоследствии вы можете указывать и другие соединения для управления другими облачными сегментами.

   Если вы выбрали Azure, укажите следующие параметры:

   - **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".

- **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 в 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.

- **Имя учетной записи хранения Azure**

  Вы создали имя учетной записи хранения Azure для работы с Kaspersky Security Center.

- **Ключ доступа хранилища Azure**

  Вы получили пароль (ключ) при создании учетной записи хранения Azure для работы с Kaspersky Security Center.

  Ключ доступен в разделе "Overview of the Azure storage account" в подразделе "Keys".

Если вы выбрали Google Cloud, укажите следующие параметры:

- **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".

- **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.

5. Если вы хотите, выберите **Настроить расписание опроса** и измените параметры заданные 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 соединений 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 AWS IAM-пользователю с другим ключом.

Чтобы удалить соединение:

1. В дереве консоли выберите узел **Обнаружение устройств → Cloud**.
2. В рабочей области окна выберите **Настроить параметры опроса**.

   Появится окно со списком соединений, используемых для опроса облачных сегментов.
3. Выделите соединение, которое вы хотите удалить, и нажмите на кнопку **Удалить** в правой части окна.
4. В появившемся окне нажмите на кнопку **OK**, чтобы подтвердить свой выбор.

Если вы удаляете соединение из списка доступных, то устройства, находящиеся внутри соответствующих сегментов, автоматически удалятся из соответствующих групп администрирования.

Настройка расписания опроса

Опрос облачного сегмента происходит по расписанию. Вы можете задать периодичность, с которой происходит опрос.

В параметрах мастера настройки облачного окружения автоматически задается периодичность опроса – раз в 5 минут. Вы можете изменить это значение в любое время и задать другое расписание. Не рекомендуется производить опрос чаще, чем раз в 5 минут, так как это может привести к ошибкам в работе API.

Чтобы настроить расписание опроса облачного сегмента:

1. В дереве консоли выберите узел **Обнаружение устройств → Cloud**.
2. В рабочей области нажмите **Настроить параметры опроса**.

   Откроется окно свойств объекта.
3. В списке выберите необходимое соединение нажмите на кнопку **Свойства**.

   Откроется окно свойств соединения.
4. В окне свойств перейдите по ссылке **Настроить расписание опроса**.

   Отобразится окно **Расписание**.

5. Настройте 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.

- **Запускать пропущенные задачи**

  Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

  Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

  Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

  По умолчанию параметр включен.

6. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Расписание опроса настроено и сохранено.

Установка приложений на устройства в облачном окружении

Вы можете установить на устройства в облачном окружении следующие приложения "Лаборатории Касперского": Kaspersky Security для Windows Server (для устройств с операционной системой Windows) и Kaspersky Endpoint Security для Linux (для устройств с операционной системой Linux).

Клиентские устройства, на которые вы планируете устанавливать защиту, должны соответствовать требованиям, установленным для работы Kaspersky Security Center в облачном окружении. У вас должна быть действующая лицензия для установки приложений на инстансы AWS, на виртуальные машины Microsoft Azure или на инстансы виртуальных машин Google.

Kaspersky Security Center 15.1 поддерживает следующие сценарии:

- Клиентское устройство обнаружено с помощью API; установка также выполняется средствами API. Этот сценарий поддерживается для облачного окружения AWS и Azure.
- Клиентское устройство обнаружено с помощью опроса Active Directory, Windows-доменов или IP-диапазонов; установка выполняется средствами Kaspersky Security Center.
- Клиентское устройство обнаружено с помощью Google API; установка выполняется средствами Kaspersky Security Center. Этот сценарий поддерживается только для Google Cloud.

Другие способы установки приложений не поддерживаются.

Для установки приложений на виртуальные устройства используйте инсталляционные пакеты.

Чтобы создать задачу удаленной установки приложения на инстансы средствами AWS API или Azure API:

1. В дереве консоли выберите папку **Задачи**.
2. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. В окне **Выбор типа задачи** выберите тип задачи **Удаленная установка приложения**.
4. В окне **Выбор устройств** выберите нужные устройства из группы **Управляемые устройства\Cloud**.
5. Если на устройствах, на которые вы планируете установить приложение, еще не установлен Агент администрирования, на странице **Выбор учетной записи для запуска задачи** выберите пункт **Учетная запись требуется (Агент администрирования не используется)** и нажмите на кнопку **Добавить** в правой части окна. В появившемся меню выберите:

   - **Учетная запись облачного сегмента**

     Выберите этот параметр, если вы хотите установить приложения на инстансы в среде AWS и получить ключ доступа AWS IAM с требуемыми правами, но не иметь IAM-роли. Также выберите этот параметр, если вы хотите установить приложения на устройства в среде Azure.

     В появившемся окне предоставьте Kaspersky Security Center учетные данные, дающие право на установку приложений на необходимые вам устройства.

     Выберите облачное окружение AWS или Azure.

     В поле **Имя учетной записи** введите имя для этих учетных данных. Это имя отображается в списке учетных записей для запуска задачи.

     Если вы выбрали AWS, в полях **ID ключа доступа** и **Секретный ключ** введите учетные данные IAM-пользователя, у которого есть права на установку приложений на указанных устройствах.

     Если вы выбрали Azure, в полях **Идентификатор подписки Azure** и **Пароль приложения в Azure** введите данные учетной записи Azure, у которой есть права на установку приложений на указанных устройствах.

     Если вы укажете неправильные учетные данные, задача удаленной установки приложений закончится ошибкой на устройствах, для которых она запланирована.

- **Учетная запись.**

  Для инстансов с операционной системой Windows выберите этот параметр, в случае если вы не будете устанавливать приложение с использованием инструментов AWS или Azure API. В этом случае убедитесь, что устройства в вашем облачном сегменте соответствуют необходимым условиям. Kaspersky Security Center выполнит установку приложений собственными средствами без использования AWS API или Azure API.

  Если вы укажете неправильные данные, задача удаленной установки приложений закончится ошибкой на устройствах, для которых она запланирована.

- **IAM-роль**

  Выберите этот параметр, если вы хотите установить приложения на инстансы в окружении AWS и иметь IAM-роль с требуемыми правами.

  Если вы выберете этот параметр, у вас не будет IAM-роли с требуемыми правами и задача удаленной установки приложений завершится с ошибкой на устройствах, для которых она запланирована.

- **SSH сертификат**

  Для инстансов с операционной системой Linux выберите этот параметр в случае, если вы не будете устанавливать приложение с использованием инструментов AWS API или Azure API. В этом случае убедитесь, что устройства в вашем облачном сегменте соответствуют необходимым условиям. Kaspersky Security Center выполнит установку приложений собственными средствами без использования AWS API или Azure API.

  Чтобы указать закрытый ключ SSH-сертификата, вы можете сгенерировать его с помощью утилиты ssh-keygen. Обратите внимание, что Kaspersky Security Center поддерживает формат закрытых ключей PEM, а утилита ssh-keygen по умолчанию генерирует SSH-ключи в формате OPENSSH. Формат OPENSSH не поддерживается Kaspersky Security Center. Чтобы создать закрытый ключ в поддерживаемом формате PEM, добавьте параметр `-m PEM` в команду ssh-keygen. Например:

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "<электронная почта пользователя>"
  ```

Вы можете предоставить несколько учетных данных, каждый раз нажимая на кнопку **Добавить**. Если разные облачные сегменты требуют разных учетных данных, укажите учетные данные для всех сегментов.

Задача удаленной установки приложения появится в списке задач в рабочей области папки **Задачи**.

В Microsoft Azure удаленная установка приложений безопасности на виртуальную машину может привести к удалению настраиваемого расширения скриптов, установленного на этой виртуальной машине.

Просмотр свойств облачных устройств

Чтобы просмотреть свойства облачного устройства:

1. В дереве консоли в папке **Обнаружение устройств** → **Cloud** выберите папку, соответствующую той группе, в которой находится интересующий вас инстанс.

Если вы не знаете, в какой группе находится нужное вам виртуальное устройство, воспользуйтесь поиском:

a. Нажмите правой кнопкой мыши на узел **Управляемые устройства** → **Cloud** и в контекстном меню выберите пункт **Поиск**.

b. В появившемся окне выполните поиск.

Если устройство, соответствующее введенным критериям, существует, то его имя и информация о нем будут отображены в нижней части окна.

2. Нажмите на название нужного узла правой клавишей мыши. В контекстном меню выберите пункт **Свойства**.

В появившемся окне отобразятся свойства объекта.

В разделе **Информация о системе** → **Общая информация о системе** содержатся параметры, которые специфичны для устройств в облачном окружении:

- **Устройство обнаружено с помощью API** (**AWS**, **Azure** или **Google Cloud**; если устройство не может быть обнаружено с помощью инструментов API, отображается значение **Нет**).
- **Облачный регион**.
- **Cloud VPC** (только для устройств AWS и Google Cloud).
- **Облачная зона доступности** (только для устройств AWS и Google Cloud).
- **Облачная подсеть**.
- **Облачная группа размещения** (это устройство отображается, если инстанс принадлежит группе размещения; в противном случае свойство не отображается).

Чтобы экспортировать эту информацию в файл формата CSV или TXT, нажмите на кнопку **Экспортировать в файл**.

Синхронизация с облачным окружением

Во время настройки облачного окружения автоматически создается правило Синхронизация с облачным окружением. Правило позволяет автоматически перемещать инстансы, найденные при каждом опросе, из группы **Нераспределенные устройства** в группу **Управляемые устройства****Cloud**, чтобы инстансы 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. Нажмите правой клавишей мыши на название узла **Обнаружение устройств** в дереве консоли.
2. В контекстном меню выберите пункт **Свойства**.
3. В открывшемся окне **Свойства** в панели **Разделы** выберите раздел **Перемещение устройств**.
4. В списке правил перемещения устройств выберите **Синхронизация с облачным окружением** и нажмите на кнопку **Свойства** внизу окна.

Откроется окно свойств правила.

5. При необходимости укажите следующие параметры в блоке параметров **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 из вложенных объектов 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 на этапе настройки облачного окружения вы включили параметр **Синхронизация с облачным окружением**, то правило Синхронизация с облачным окружением создается с установленными флажками **Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств** и **Удалять подгруппы, для которых нет соответствия в облачных сегментах**.

  Если вы не включили параметр **Синхронизация с облачным окружением**, правило будет создано с выключенным параметром. Если в процессе работы с Kaspersky Security Center вам потребуется, чтобы структура подгрупп внутри подгруппы **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.

6. Выберите значение в раскрывающемся списке **Устройство обнаружено 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.
    - **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.
7. **Не задано**. Это условие не применяется. При необходимости настройте другие свойства правила в других разделах.
8. При необходимости применить правило, нажав на кнопку **Выполнить сейчас** внизу окна.

    Будет запущен мастер выполнения правила. Следуйте далее указаниям мастера. После окончания работы мастера правило будет запущено и структура групп внутри подгруппы **Управляемые устройства\Cloud** будет соответствовать структуре ваших облачных сегментов.
9. Нажмите на кнопку **OK**.

Параметры настроены и сохранены.

Чтобы выключить правило Синхронизация с Cloud:

1. Нажмите правой клавишей мыши на название узла **Обнаружение устройств** в дереве консоли.
2. В контекстном меню выберите пункт **Свойства**.
3. В открывшемся окне **Свойства** в панели **Разделы** выберите раздел **Перемещение устройств**.
4. В списке правил перемещения устройств выключите параметр **Синхронизация с облачным окружением** и нажмите на кнопку **OK**.

Правило выключено и больше не применяется.

Схема работы Kaspersky Security Center в Yandex.Cloud

Вы можете развернуть Kaspersky Security Center в Yandex.Cloud. Доступен только режим оплаты по факту использования; облачные базы данных не поддерживаются.

В Yandex.Cloud доступны следующие способы развертывания приложений безопасности:

- Собственными средствами Kaspersky Security Center, то есть с помощью задачи *Удаленная установка* (развертывание приложений безопасности возможно только в том случае, если Сервер администрирования и защищаемые виртуальные машины находятся в одном сегменте сети).
- С помощью скриптов развертывания

Для развертывания Kaspersky Security Center в Yandex.Cloud у вас должна быть учетная запись в Yandex.Cloud. Вам нужно предоставить этой учетной записи разрешение marketplace.meteringAgent и связать эту учетную запись с виртуальной машиной (подробности см. на странице https://cloud.yandex.ru).

Приложения

В этом разделе содержится справочная и дополнительная информация, касающаяся использования Kaspersky Security Center.

Дополнительные возможности

В этом разделе рассматривается ряд дополнительных функций приложения Kaspersky Security Center, предназначенных для расширения возможностей централизованного управления приложениями на устройствах.

Автоматизация работы Kaspersky Security Center. Утилита klakaut

Вы можете автоматизировать работу Kaspersky Security Center с помощью утилиты klakaut. Утилита klakaut и справочная система для нее расположены в папке установки Kaspersky Security Center.

Работа с внешними инструментами

Kaspersky Security Center позволяет сформировать список *внешних инструментов* (далее также *инструментов*) – приложений, которые вызываются для клиентского устройства из Консоли администрирования при помощи группы контекстного меню **Внешние инструменты**. Для каждого инструмента из списка создается отдельная команда меню, с помощью которой Консоль администрирования запускает соответствующую инструменту приложение.

Приложение запускается на рабочем месте администратора. В качестве аргументов командной строки приложение может принимать атрибуты удаленного клиентского устройства (NetBIOS-имя, DNS-имя, IP-адрес). Подключение к удаленному устройству может выполняться при помощи туннелированного соединения.

По умолчанию для каждого клиентского устройства список внешних инструментов содержит следующие сервисные приложения:

- **Удаленная диагностика** – утилита удаленной диагностики Kaspersky Security Center.
- **Удаленный рабочий стол** – стандартный компонент Microsoft Windows "Подключение к удаленному рабочему столу".
- **Управление компьютером** – стандартный компонент Microsoft Windows.

Чтобы добавить или удалить внешние инструменты, а также изменить их параметры,

В контекстном меню выбранного устройства выберите пункт **Внешние инструменты → Настроить внешние инструменты**.

Откроется окно **Внешние инструменты**. В этом окне можно добавлять внешние инструменты или изменять их параметры с помощью кнопок **Добавить** и **Изменить**. Чтобы удалить внешние инструменты, нажмите на кнопку удаления со значком красного крестика ( ).

Режим клонирования диска Агента администрирования

Клонирование жесткого диска "эталонного" устройства является распространенным способом установки программного обеспечения на новые устройства. Если Агент администрирования на жестком диске "эталонного" устройства во время клонирования работает в обычном режиме, возникает следующая проблема:

После развертывания на новых устройствах эталонного образа диска с Агентом администрирования эти устройства отображаются в Консоли администрирования одним значком. Проблема возникает потому, что при клонировании на новых устройствах сохраняются одинаковые внутренние данные, позволяющие Серверу администрирования связать устройство со значком в Консоли администрирования.

Избежать проблемы с неверным отображением новых устройств в Консоли администрирования после клонирования помогает специальный *режим клонирования диска Агента администрирования*. Используйте этот режим, если вы разворачиваете программное обеспечение (с Агентом администрирования) на новых устройствах путем клонирования диска.

В режиме клонирования диска Агент администрирования работает, но не подключается к Серверу администрирования. При выходе из режима клонирования Агент администрирования удаляет внутренние данные, из-за наличия которых Сервер администрирования связывает несколько устройств с одним значком в Консоли администрирования. По завершении клонирования образа "эталонного" устройства, новые устройства отображаются в Консоли администрирования нормально (отдельными значками).

Сценарий использования режима клонирования диска Агента администрирования

1. Администратор устанавливает Агент администрирования на "эталонном" устройстве.
2. Администратор проверяет подключение Агента администрирования к Серверу администрирования с помощью утилиты klnagchk.
3. Администратор включает режим клонирования диска Агента администрирования.
4. Администратор устанавливает на устройство программное обеспечение, патчи и выполняет любое количество перезагрузок устройства.
5. Администратор выполняет клонирование жесткого диска "эталонного" устройства на любое число устройств.

6. Для каждой клонированной копии должны быть выполнены следующие условия:

   a. имя устройства изменено;

   b. устройство перезагружено;

   c. режим клонирования диска выключен.

Включение и выключение режима клонирования диска с помощью утилиты klmover

Чтобы включить или выключить режим клонирования диска Агента администрирования:

1. Запустите утилиту klmover на устройстве с установленным Агентом администрирования, который нужно клонировать.

   Утилита klmover находится в папке установки Агента администрирования.

2. Чтобы включить режим клонирования диска, в командной строке Windows введите команду:

   ```
   klmover -cloningmode 1
   ```

   Агент администрирования переключается в режим клонирования диска.

3. Чтобы запросить текущее состояние режима клонирования диска, в командной строке введите команду:

   ```
   klmover -cloningmode
   ```

   В результате в окне утилиты отобразится информация о том, включен или выключен режим клонирования диска.

4. Чтобы выключить режим клонирования диска, в командной строке утилиты введите команду:

   ```
   klmover -cloningmode 0
   ```

Подготовка эталонного устройства с установленным Агентом администрирования для создания образа операционной системы

Вы можете создать образ операционной системы эталонного устройства с установленным Агентом администрирования, а затем развернуть образ на сетевых устройствах. В этом случае вы создаете образ операционной системы эталонного устройства, на котором Агент администрирования еще не запущен. Если вы запустите Агент администрирования на эталонном устройстве до создания образа операционной системы, идентификация Сервера администрирования устройств, развернутых из образа операционной системы эталонного устройства, будет проблематичной.

Чтобы подготовить эталонное устройство для создания образа операционной системы:

1. Убедитесь, что операционная система Windows установлена на эталонном устройстве, также установите другое программное обеспечение, которое вам нужно на этом устройстве.

2. На эталонном устройстве в параметрах сетевых подключений Windows отключите эталонное устройство от сети, в которой установлен Kaspersky Security Center.

3. На эталонном устройстве запустите локальную установку Агента администрирования с помощью файла setup.exe.

   Запускается мастер установки Агента администрирования Kaspersky Security Center. Следуйте далее указаниям мастера.

4. На странице **Сервера администрирования** мастера укажите IP-адрес Сервера администрирования.

   Если вы не знаете точный адрес Сервера администрирования, введите localhost. Вы можете изменить IP-адрес позже, используя утилиту klmover с ключом `-address`.

5. На странице **Запустить приложение** в мастере отключите параметр **Запустить приложение в процессе установки**.

6. После завершения установки Агента администрирования не перезагружайте устройство перед созданием образа операционной системы.

   Если вы перезагрузите устройство, вам нужно будет повторить весь процесс подготовки эталонного устройства для создания образа операционной системы.

7. На эталонном устройстве в командной строке запустите утилиту sysprep и выполните следующую команду: `sysprep.exe /generalize /oobe /shutdown`.

Эталонное устройство готово к созданию образа операционной системы.

Настройка параметров получения сообщений от компонента Мониторинг файловых операций

Управляемые приложения, такие как Kaspersky Security для Windows Server или Kaspersky Security для виртуальных сред Легкий агент, отправляют сообщения компонента Мониторинг файловых операций в Kaspersky Security Center. Kaspersky Security Center также позволяет отслеживать любые изменения критически важных компонентов систем (таких как веб-серверы и банкоматы) и оперативно реагировать на нарушения целостности таких систем. Для этого реализована поддержка получения сообщений от компонента Мониторинг файловых операций. Компонент Мониторинг файловых операций позволяет следить не только за файловой системой устройства, но и за ветками реестра, состоянием сетевого экрана и состоянием подключенного оборудования.

Требуется выполнить настройку Kaspersky Security Center, чтобы получать сообщения от компонента Мониторинг файловых операций без использования приложений Kaspersky Security для Windows Server или Kaspersky Security для виртуальных сред Легкий агент.

Чтобы настроить параметры получения сообщений от компонента Мониторинг файловых операций:

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.

2. Перейдите в раздел:

   - для 32-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

   - для 64-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF

3. Создайте ключи:

- Создайте ключ KLSRV_EVP_FIM_PERIOD_SEC, чтобы указать интервал времени подсчета числа обработанных событий. Задайте следующие параметры:

  a. Укажите название ключа KLSRV_EVP_FIM_PERIOD_SEC.

  b. Укажите тип ключа DWORD.

  c. Задайте диапазон значений промежутка времени от 43 200 до 172 800 секунд. По умолчанию промежуток проверки равен 86 400 секунд.

- Создайте ключ KLSRV_EVP_FIM_LIMIT для ограничения количества принимаемых событий за указанный промежуток времени. Задайте следующие параметры:

  a. Укажите название ключа KLSRV_EVP_FIM_LIMIT.

  b. Укажите тип ключа DWORD.

  c. Задайте диапазон значений принимаемых событий от 2000 до 50 000. По умолчанию количество событий равно 20 000.

- Создайте ключ KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC для подсчета событий с точностью до определенного промежутка времени. Задайте следующие параметры:

  a. Укажите название ключа KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC.

  b. Укажите тип ключа DWORD.

  c. Задайте диапазон значений от 120 до 600 секунд. Временной интервал, установленный по умолчанию, составляет 300 секунд.

- Создайте ключ KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC, чтобы после указанного значения времени приложение выполняло проверку того, что число событий, обработанных за промежуток времени, становится меньше заданного ограничения. Проверка выполняется при достижении ограничения приема событий. Если условие выполняется, возобновляется сохранение событий в базу данных. Задайте следующие параметры:

  a. Укажите название ключа KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC.

  b. Укажите тип ключа DWORD.

  c. Задайте диапазон значений от 600 до 3600 секунд. Временной интервал, установленный по умолчанию, составляет 1800 секунд.

Если ключи не созданы, используются значения по умолчанию.

4. Перезапустите службу Сервера администрирования.

Ограничения получения событий от компонента Мониторинга файловых операций будут настроены. Результаты работы компонента Мониторинг файловых операций можно посмотреть в отчетах **Топ 10 правил Мониторинга файловых операций / Контроля целостности системы, наиболее часто срабатывающие на устройствах** и **Топ 10 устройств с правилами Мониторинга файловых операций / Контроля целостности системы, срабатывающими чаще всего**.

Обслуживание Сервера администрирования

Обслуживание Сервера администрирования позволяет освободить место в папке Сервера администрирования и уменьшить объем базы данных за счет удаления ненужных объектов. Это поможет вам повысить производительность и надежность работы приложения. Рекомендуется выполнять обслуживание Сервера администрирования не реже одного раза в неделю.

Обслуживание Сервера администрирования выполняется с помощью соответствующей задачи. Во время обслуживания Сервера администрирования приложение выполняет следующие действия:

- Удаляет ненужные папки и файлы из папки хранилища.
- Удаляет ненужные записи из таблиц (также известные как "висячие указатели").
- Очищает кеш.
- Обслуживает базу данных (если вы используете SQL Server или PostgreSQL в качестве СУБД):
  - проверяет базу данных на наличие ошибок (доступно только для SQL Server);
  - перестраивает индексы базы данных;
  - обновляет статистику базы данных;
  - сжимает базу данных (если необходимо).

Чтобы создать задачу Обслуживание Сервера администрирования:

1. В дереве консоли выберите узел Сервера администрирования, для которого нужно создать задачу *Обслуживание Сервера администрирования*.
2. Выберите папку **Задачи**.
3. В рабочей области папки **Задачи** нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи.
4. В окне мастера **Выбор типа задачи** выберите тип задачи **Обслуживание Сервера администрирования** и нажмите на кнопку **Далее**.
5. Если во время обслуживания нужно сжимать базу данных Сервера администрирования, в окне мастера **Параметры** установите флажок **Сжать базу данных**.
6. Следуйте дальнейшим шагам мастера.

Созданная задача отображается в списке задач в рабочей области папки **Задачи**. Для одного Сервера администрирования может выполняться только одна задача *Обслуживание Сервера администрирования*. Если задача *Обслуживание Сервера администрирования* для Сервера администрирования уже создана, создание еще одной задачи *Обслуживание Сервера администрирования* невозможно.

Доступ к общедоступным DNS-серверам

Если доступ к серверам "Лаборатории Касперского" через системный DNS невозможен, Kaspersky Security Center может использовать публичные DNS-серверы в следующем порядке:

1. Google Public DNS (8.8.8.8)
2. Cloudflare DNS (1.1.1.1)
3. Alibaba Cloud DNS (223.6.6.6)
4. Quad9 DNS (9.9.9.9)
5. CleanBrowsing (185.228.168.168)

Запросы к этим DNS-серверам могут содержать доменные адреса и общедоступный IP-адрес Сервера администрирования, так как приложение устанавливает TCP/UDP-соединение с DNS-сервером. Если Kaspersky Security Center использует общедоступный DNS-сервер, обработка данных регулируется политикой конфиденциальности соответствующего сервиса.

Чтобы настроить использование публичного DNS с помощью утилиты klscflag:

1. Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
2. Чтобы выключить использование публичного DNS, выполните следующую команду:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. Чтобы включить использование публичного DNS, выполните команду:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

Окно Способ уведомления пользователей

В окне **Способ уведомления пользователей** можно настроить параметры уведомления пользователя об установке сертификата на мобильное устройство:

- **Показать QR-код в мастере**. При выборе этого варианта ссылка на инсталляционный пакет будет отображена на последнем шаге работы мастера подключения устройства.
- **Отправить QR-код пользователю**. При выборе этого варианта вы можете настроить параметры оповещения пользователя о подключении устройства.

В блоке параметров **По электронной почте** вы можете настроить параметры уведомления пользователя об установке сертификата на его мобильное устройство с помощью сообщений электронной почты. Этот способ оповещения доступен, только если настроен SMTP-сервер.

В блоке параметров **С помощью SMS** вы можете настроить параметры уведомления пользователя об установке сертификата на его мобильное устройство с помощью SMS-сообщений. Этот способ оповещения доступен, только если настроено SMS-оповещение.

По ссылке **Изменить сообщение** в блоках параметров **По электронной почте** и **С помощью SMS** просмотрите и при необходимости отредактируйте текст уведомления.

Окно Выборка устройств

В этом окне можно указать выборку устройств, сведения о которых будут отображаться в рабочей области на закладке **Статистика** узла **Отчеты и уведомления**.

Выберите выборку из списка **Выборка устройств**. В списке перечислены выборки, заданные по умолчанию, и выборки, созданные пользователем.

Окно Определение названия создаваемого объекта

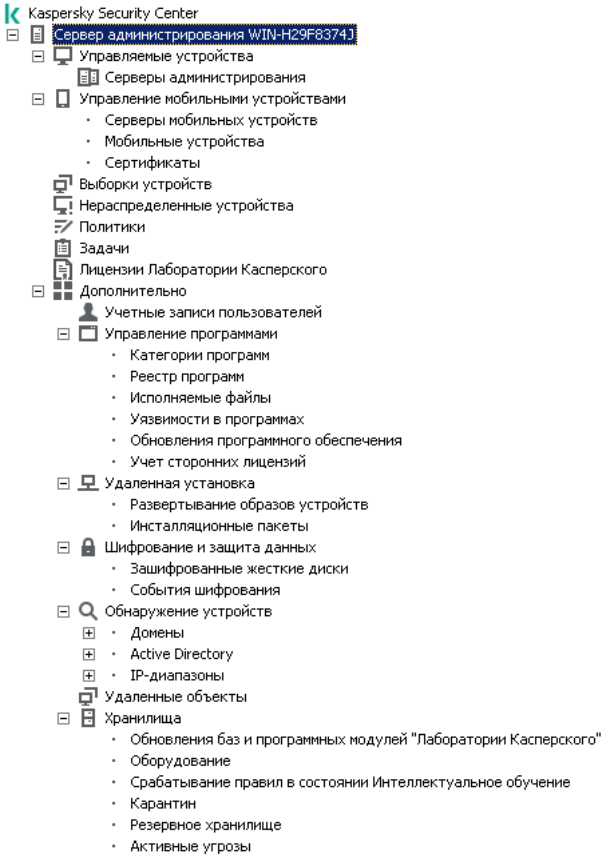
В окне укажите название создаваемого объекта. Имя не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

Особенности работы с интерфейсом управления

Этот раздел содержит описание приемов работы в главном окне Kaspersky Security Center.

Дерево консоли

Дерево консоли (см. рис. ниже) предназначено для отображения сформированной в сети иерархии Серверов администрирования, структуры их групп администрирования, а также других объектов приложения (например, папок **Хранилища** и **Управление приложениями**). Пространство имен Kaspersky Security Center может содержать несколько узлов с именами серверов, соответствующих установленным и включенным в структуру сети Серверам администрирования.



Дерево консоли

Узел Сервер администрирования

Узел **Сервер администрирования – <Имя устройства>** является контейнером и отображает структурную организацию указанного Сервера администрирования.

В рабочей области узла **Сервер администрирования** содержится сводная информация о текущем состоянии приложения и устройств, находящихся под управлением Сервера администрирования. Информация в рабочей области распределена по вкладкам:

- **Мониторинг**. На вкладке Мониторинг в реальном времени отображается информация о работе приложения и текущем состоянии клиентских устройств. Важные сообщения для администратора (например, сообщения об уязвимостях, ошибках, обнаружении вирусов) выделяются цветом. По ссылкам на вкладке **Мониторинг** можно выполнять типовые задачи администратора (например, установить и настроить приложение безопасности на клиентских устройствах), а также переходить к другим папкам дерева консоли.

- **Статистика**. Содержит набор диаграмм, сгруппированных по темам (состояние защиты, антивирусная статистика, обновления и прочее). В диаграммах в визуальной форме представлена текущая информация о работе приложения и состоянии клиентских устройств.

- **Отчеты**. Содержит шаблоны отчетов, формируемых приложением. На вкладке вы можете формировать отчеты из предустановленных шаблонов, а также создавать собственные шаблоны отчетов.

- **События**. Содержит записи о событиях, зарегистрированных во время работы приложения. Для удобства чтения и сортировки записи распределены по тематическим выборкам. На вкладке вы можете просмотреть выборки событий, сформированные автоматически, а также создать собственные выборки.

Папки в составе узла Сервер администрирования

В состав узла **Сервер администрирования – <Имя устройства>** входят следующие папки:

- **Управляемые устройства**. Папка предназначена для хранения, отображения, настройки и изменения структуры групп администрирования, групповых политик и групповых задач.

- **Управление мобильными устройствами**. Папка предназначена для управления мобильными устройствами. Папка **Управление мобильными устройствами** содержит следующие вложенные папки:

  - **Серверы мобильных устройств**. Предназначен для управления Серверами iOS MDM.

  - **Мобильные устройства**. Предназначена для управления мобильными устройствами KES и iOS MDM.

  - **Сертификаты**. Предназначена для управления сертификатами мобильных устройств.

- **Выборки устройств**. Папка предназначена для быстрого выбора устройств, соответствующих определенным критериям (выборки устройств), среди всех управляемых устройств. Например, вы можете быстро выбрать устройства, на которых не установлено приложение безопасности, и перейти к этим устройствам (просмотреть их список). С выбранными устройствами можно выполнять действия, например, назначать для них задачи. Вы можете использовать предустановленные выборки, а также создавать собственные (пользовательские) выборки.

- **Нераспределенные устройства**. В папке содержится список устройств, не входящих ни в одну группу администрирования. Вы можете выполнять действия с нераспределенными устройствами, например, перемещать их в группы администрирования, устанавливать на них приложения.

- **Политики**. Папка предназначена для просмотра и создания политик.

- **Задачи**. Папка предназначена для просмотра и создания задач.

- **Лицензии "Лаборатории Касперского"**. Содержит список доступных лицензионных ключей для приложений "Лаборатории Касперского". В рабочей области папки вы можете добавлять новые лицензионные ключи в хранилище лицензионных ключей, распространять лицензионные ключи на управляемые устройства, просматривать отчет об использовании лицензионных ключей.

- **Дополнительно**. Папка содержит набор вложенных папок, соответствующих различным группам функциональностей приложения.

Папка Дополнительно. Перемещение папок в дереве консоли

В состав папки **Дополнительно** входят следующие папки:

- **Учетные записи пользователей**. Папка содержит список учетных записей пользователей сети.

- **Управление приложениями**. Папка предназначена для управления приложениями, установленными на устройствах в сети. Папка **Управление приложениями** содержит следующие вложенные папки:

  - **Категории приложений**. Предназначена для работы с пользовательскими категориями приложений.

  - **Реестр приложений**. Содержит список приложений на устройствах с установленным Агентом администрирования.

  - **Исполняемые файлы**. Содержит список исполняемых файлов, хранящихся на клиентских устройствах с установленным Агентом администрирования.

  - **Уязвимости в приложениях**. Содержит список уязвимостей в приложениях на устройствах с установленным Агентом администрирования.

  - **Обновления программного обеспечения**. Содержит список обновлений приложений, полученных Сервером администрирования, которые могут быть распространены на устройства.

  - **Учет сторонних лицензий**. Содержит список групп лицензионных приложений. С помощью групп лицензионных приложений можно отслеживать использование лицензий на сторонние приложения (не приложения "Лаборатории Касперского") и нарушение лицензионных ограничений.

- **Удаленная установка**. Папка предназначена для управления удаленной установкой операционных систем и приложений. Папка **Удаленная установка** содержит следующие вложенные папки:

  - **Развертывание образов устройств**. Предназначена для развертывания образов операционных систем на устройствах.

  - **Инсталляционные пакеты**. Содержит список инсталляционных пакетов, которые могут использоваться для удаленной установки приложений на устройства.

- **Шифрование и защита данных**. Папка предназначена для управления процессом шифрования данных на жестких и съемных дисках.

- **Опрос сети**. Папка предназначена для отображения сети, в которой установлен Сервер администрирования. Информацию о структуре сети и входящих в ее состав устройствах Сервер администрирования получает в ходе регулярных опросов сети Windows, IP-диапазонов и Active Directory, сформированных в сети организации. Результаты опросов отображаются в рабочих областях соответствующих папок: **Домены**, **IP-диапазоны** и **Active Directory**.

- **Хранилища**. Папка предназначена для работы с объектами, которые используются для мониторинга состояния устройств и их обслуживания. Папка **Хранилища** содержит следующие вложенные папки:

  - **Срабатывание правил в состоянии Интеллектуальное обучение**. Содержит список обнаружений, выполняемых правилами Kaspersky Endpoint Security, работающими в режиме Интеллектуального обучения на клиентских устройствах.

  - **Обновления и патчи ПО "Лаборатории Касперского"**. Содержит список обновлений, полученных Сервером администрирования, которые могут быть распространены на устройства.

  - **Оборудование**. Содержит список оборудования, подключенного к сети организации.

  - **Карантин**. Содержит список объектов, помещенных антивирусными приложениями в карантинные папки на устройствах.

  - **Резервное хранилище**. Папка содержит список резервных копий файлов, удаленных или измененных в процессе лечения на устройствах.

  - **Необработанные файлы**. Содержит список файлов, для которых приложения безопасности определили необходимость отложенного лечения.

Вы можете изменять набор папок, вложенных в папку **Дополнительно**. Вложенные папки, которые активно используются, можно перемещать из папки **Дополнительно** на уровень выше. Папки, которые используются в работе редко, можно помещать в папку **Дополнительно**.

*Чтобы переместить из папки **Дополнительно** вложенную папку:*

1. В дереве консоли выберите вложенную папку, которую вы хотите переместить из папки **Дополнительно**.
2. В контекстном меню вложенной папки выберите пункт **Вид** → **Переместить из папки Дополнительно**.

Вы также можете вынести вложенную папку из папки **Дополнительно** в рабочей области папки **Дополнительно**, по ссылке **Переместить из папки Дополнительно** в блоке с названием вложенной папки.

*Чтобы переместить папку в папку **Дополнительно**:*

1. В дереве консоли выберите папку, которую нужно переместить в папку **Дополнительно**.
2. В контекстном меню папки выберите пункт **Вид** → **Переместить в папку Дополнительно**.

Как обновить данные в рабочей области

В Kaspersky Security Center данные рабочей области (такие как статусы устройств, статистика и отчеты) никогда не обновляются автоматически.

Чтобы обновить данные в рабочей области, выполните одно из следующих действий:

- нажмите на клавишу **F5**;
- в контекстном меню объекта в дереве консоли выберите пункт **Обновить**;
- Нажмите на значок обновления () в рабочей области.

Как перемещаться по дереву консоли

Для перемещения по дереву консоли вы можете использовать следующие кнопки, расположенные в панели инструментов:

-  – переход на один шаг назад;
-  – переход на один шаг вперед;
-  – переход на один уровень вверх.

Можно также воспользоваться навигационной цепочкой, расположенной в правом верхнем углу рабочей области. Навигационная цепочка содержит полный путь к той папке дерева консоли, в которой вы находитесь в текущий момент. Все элементы цепочки, кроме последнего, являются ссылками на объекты дерева консоли.

Как открыть окно свойств объекта в рабочей области

Свойства большинства объектов Консоли администрирования можно изменять в окне свойств объекта.

Чтобы открыть окно свойств объекта, расположенного в рабочей области, выполните одно из следующих действий:

- в контекстном меню объекта выберите пункт **Свойства**;
- выберите объект и нажмите комбинацию клавиш **ALT+ENTER**.

Как выбрать группу объектов в рабочей области

Вы можете выбрать группу объектов в рабочей области. Выбор группы объектов можно использовать, например, для создания набора устройств и последующего формирования задач для него.

Чтобы выбрать диапазон объектов:

1. Выберите первый объект диапазона и нажмите на клавишу **SHIFT**.
2. Удерживая нажатой клавишу **SHIFT**, выберите последний объект диапазона.

   Диапазон будет выбран.

Чтобы объединить отдельные объекты в группу:

1. Выберите первый объект в составе группы и нажмите на клавишу **CTRL**.
2. Удерживая нажатой клавишу **CTRL**, выберите остальные объекты группы.

Объекты будут объединены в группу.

Как изменить набор граф в рабочей области

Консоль администрирования позволяет изменять набор граф, отображаемых в рабочей области.

Чтобы изменить набор граф в рабочей области:

1. Выберите объект дерева консоли, для которого вы хотите изменить набор граф.
2. В рабочей области папки откройте окно настройки набора граф по ссылке **Добавить или удалить столбцы**.
3. В окне **Добавить или удалить столбцы** сформируйте набор граф для отображения.

Справочная информация

В этом разделе в таблицах представлена сводная информация о контекстном меню объектов Консоли администрирования, а также о статусах объектов дерева консоли и рабочей области.

Команды контекстного меню

В этом разделе содержится перечень объектов Консоли администрирования и соответствующий им набор пунктов контекстного меню (см. таблицу ниже).

Элементы контекстного меню объектов Консоли администрирования

Объект	Пункт меню	Назначение пункта меню
Общие пункты контекстного меню	**Поиск**	Открыть окно поиска устройств.
	Обновить	Обновить отображение выбранного объекта.
	Экспортировать список	Экспортировать текущий список в файл.
	Свойства	Открыть окно свойств выбранного объекта.
	Вид → Добавить или удалить столбцы	Добавить или удалить графы в таблице объектов в рабочей области.
	Вид → Крупные значки	Отображать объекты в рабочей области в виде крупных значков.
	Вид → Мелкие значки	Отображать объекты в рабочей области в виде мелких значков.
	Вид → Список	Отображать объекты в рабочей области в виде списка.
	Вид → Таблица	Отображать объекты в рабочей области в виде таблицы.
	Вид→ Настройка интерфейса	Настроить отображение элементов Консоли администрирования.
Kaspersky Security Center	**Создать → Сервер администрирования**	Добавить в дерево консоли Сервер администрирования.
<Имя Сервера администрирования>	**Подключиться к Серверу администрирования**	Подключиться к Серверу администрирования.
	Отключиться от Сервера администрирования	Отключиться от Сервера администрирования.
Управляемые устройства	**Установить приложение**	Запустить мастер удаленной установки приложения.
	Вид → Настройка интерфейса	Настроить отображение элементов интерфейса.
	Удалить	Удалить Сервер администрирования из дерева консоли.
	Установить приложение	Запустить мастер удаленной установки для группы администрирования.
	Обнулить счетчик вирусов	Обнулить счетчики вирусов для устройств, входящих в состав группы администрирования.
	Просмотреть отчет об угрозах	Создать отчет об угрозах и вирусной активности устройств, входящих в состав группы администрирования.
	Создать → Группу	Создать группу администрирования.
	Все задачи → Новая структура групп	Создать структуру групп администрирования на основе структуры доменов или Active Directory.
	Все задачи → Показать сообщение	Запустить мастер создания сообщения для пользователей устройств, входящих в группу администрирования.
Управляемые устройства → Серверы администрирования	**Создать → Подчиненный Сервер администрирования**	Запустить мастер добавления подчиненного Сервера администрирования.
	Создать → Виртуальный Сервер администрирования	Запустить мастер создания виртуального Сервера администрирования.
Управление мобильными устройствами → Мобильные устройства	**Создать → Мобильное устройство**	Подключить новое мобильное устройство пользователя.
Управление мобильными устройствами → Сертификаты	**Создать → Сертификат**	Создать сертификат.
	Создать → Мобильное устройство	Подключить новое мобильное устройство пользователя.
Выборки устройств	**Создать → Новая выборка**	Создать выборку устройств.
	Все задачи → Импортировать	Импортировать выборку из файла.

Объект	Пункт меню	Назначение пункта меню
Лицензии "Лаборатории Касперского"	**Добавить код активации или файл ключа**	Добавить лицензионный ключ в хранилище Сервера администрирования.
	Активировать приложение	Запустить мастер создания задачи активации приложения.
	Отчет об использовании лицензионных ключей	Создать и просмотреть отчет о лицензионных ключах на клиентских устройствах.
Управление приложениями → Категории приложений	**Создать → Категорию**	Создать категорию приложений.
Управление приложениями → Реестр приложений	**Фильтр**	Настроить фильтр для списка приложений.
	Наблюдаемые приложения	Настроить публикацию событий об установке приложений.
	Удалить неустановленные приложения	Удалить из списка информацию о приложениях, которые уже не установлены на устройствах сети.
Управление приложениями → Обновления программного обеспечения	**Принять Лицензионные соглашения обновлений**	Принять Лицензионные соглашения обновлений программного обеспечения.
Управление приложениями → Учет сторонних лицензий	**Создать → Группу лицензионных приложений**	Создать группу лицензионных приложений.
Удаленная установка → Инсталляционные пакеты	**Показать текущие версии приложений**	Просмотреть список актуальных версий приложений "Лаборатории Касперского", выложенных на интернет-серверах.
	Создать → Инсталляционный пакет	Создать инсталляционный пакет.
	Все задачи → Обновить базы	Обновить базы приложений в инсталляционных пакетах.
	Все задачи → Показать общий список автономных пакетов	Просмотреть список автономных инсталляционных пакетов, созданных для инсталляционных пакетов.
Обнаружение устройств → Домены	**Все задачи → Активность устройств**	Настроить параметры реакции Сервера администрирования на отсутствие активности устройств в сети.
Обнаружение устройств → IP-диапазоны	**Создать → IP-диапазон**	Создать IP-диапазон.
Хранилища → Обновления баз и модулей приложений "Лаборатории Касперского"	**Загрузить обновления**	Открыть окно свойств задачи загрузки обновлений в хранилище Сервера администрирования.
	Параметры загрузки обновлений	Настроить параметры задачи загрузки обновлений в хранилище Сервера администрирования.
	Отчет об используемых антивирусных базах	Создать и просмотреть отчет о версиях баз.
	Все задачи → Очистить хранилище обновлений	Очистить хранилище обновлений на Сервере администрирования.
Хранилища → Оборудование	**Создать → Устройство**	Создать сетевое устройство.

Список управляемых устройств. Значение граф

В таблице ниже представлены названия и описания граф списка управляемых устройств.

Значение граф списка управляемых устройств

Название графы	Значение
Имя	NetBIOS-имя клиентского устройства. Описание значков имени устройств приведено в приложении.
Тип операционной системы	Тип операционной системы клиентского устройства.
Windows-домен	Наименование Windows-домена, в котором находится клиентское устройство.

Название графы	Значение
Агент администрирования установлен	Результат установки на клиентское устройство Агента администрирования: *Да*, *Нет*, *Нет данных*.
Агент администрирования запущен	Результат функционирования Агента администрирования: *Да*, *Нет*, *Нет данных*.
Постоянная защита	Установлено приложение безопасности: *Да*, *Нет*, *Нет данных*.
Последнее подключение к Серверу администрирования	Время, прошедшее с момента соединения клиентского устройства с Сервером администрирования.
Последнее обновление антивирусных баз	Время, прошедшее с момента последнего обновления управляемых устройств.
Статус	Текущий статус клиентского устройства: *OK*, *Критический*, *Предупреждение*.
Описание статуса	Условия изменения статуса клиентского устройства на *Критический* или *Предупреждение*. Статус устройства изменяется на *Предупреждение* или *Критический* при следующих условиях: • Приложение безопасности не установлено. • Обнаружено много вирусов. • Уровень постоянной защиты отличается от уровня, установленного администратором. • Давно не выполнялся поиск вредоносного ПО. • Базы устарели. • Давно не подключался. • Обнаружены активные угрозы. • Требуется перезагрузка. Причиной перезагрузки устройства может быть одна из следующих: ◦ Перезагружено по неизвестной причине. ◦ Приложение неработоспособно до перезагрузки. ◦ Для завершения обновления требуется Для завершения обновления требуется перезагрузка; приложение работоспособно. ◦ Для инициации обновления требуется перезагрузка. ◦ Для завершения проверки или лечения требуется перезагрузка. ◦ Требуется перезагрузка для завершения удаленной установки или удаления. ◦ Завершение шифрования данных на диске. Причины можно задать при настройке переключения статусов устройства. • Установлены несовместимые приложения. • Обнаружены уязвимости в приложениях. • Давно не выполнялась проверка обновлений Центра обновления Windows. • Недопустимый статус шифрования. • Параметры мобильного устройства не соответствуют политике. • Есть необработанные проблемы безопасности. • Статус устройства определен приложением. • На устройстве заканчивается дисковое пространство. • Срок действия лицензии скоро истекает. Статус устройства изменяется только на *Критический* по следующим причинам: • Срок действия лицензии истек. • Устройство стало неуправляемым. • Защита выключена. • Приложение безопасности не запущено. Управляемые приложения "Лаборатории Касперского" на клиентских устройствах могут пополнять список описаний статусов. Kaspersky Security Center может получать описание статуса клиентского устройства от управляемых приложений "Лаборатории Касперского", установленных на этом устройстве. Если статус, присвоенный устройству управляемыми приложениями, не совпадает со статусом, присвоенным Kaspersky Security Center, в Консоли администрирования отображается статус, наиболее критичный для безопасности устройства. Например, если одно из управляемых приложений присвоило устройству статус *Критический*, а Kaspersky Security Center – статус *Предупреждение*, то в Консоли администрирования для устройства отобразится статус *Критический* и описание этого статуса от управляемого приложения.
Информация обновлена	Время, прошедшее с момента последней успешной синхронизации клиентского устройства с Сервером администрирования (то есть с момента последнего опроса сети).
DNS-имя	Имя DNS-домена клиентского устройства.
DNS-домен	Основной DNS-суффикс.
IP-адрес	IP-адрес клиентского устройства. Рекомендовано использовать IPv4 адрес.

Название графы	Значение
Последнее появление в сети	Продолжительность видимости клиентского устройства в сети.
Последняя полная проверка	Дата и время последней проверки клиентского устройства, выполненной приложением безопасности по требованию пользователя.
Всего обнаружено угроз	Количество обнаруженных угроз.
Статус постоянной защиты	Статус постоянной защиты: *Запускается, Выполняется, Выполняется (максимальная защита), Выполняется (максимальная скорость), Выполняется (рекомендуемые параметры), Выполняется (с пользовательскими параметрами), Остановлена, Приостановлена, Сбой*.
IP-адрес соединения	IP-адрес подключения к Серверу администрирования Kaspersky Security Center.
Версия Агента администрирования	Версия Агента администрирования.
Версия приложения	Версия приложения безопасности, установленного на клиентском устройстве.
Выпуск антивирусных баз	Версия антивирусных баз.
Время начала последней сессии	Дата и время последнего включения клиентского устройства.
Требуется перезагрузка	Требуется перезагрузка клиентского устройства.
Точка распространения	Имя устройства, выполняющего роль точки распространения для этого клиентского устройства.
Описание	Описание клиентского устройства, полученное при сканировании сети.
Статус шифрования	Статус шифрования данных клиентского устройства.
Состояние WUA	Состояние Агент Центра обновления Windows клиентского устройства. Значение *Да* соответствует клиентским устройствам, которые получают обновления через Центр обновления Windows от Сервера администрирования. Значение *Нет* соответствует клиентским устройствам, которые получают обновления через Центр обновления Windows из других источников.
Архитектура операционной системы	Разрядность операционной системы клиентского устройства.
Статус защиты от спама	Статус компонента защиты от спама: *Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Нет данных*.
Статус защиты данных от утечек	Статус компонента защиты от утечки данных: *Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Нет данных*.
Статус защиты для серверов совместной работы	Статус компонента фильтрации содержимого: *Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Нет данных*.
Статус антивирусной защиты почтовых серверов	Статус компонента антивирусной защиты почтовых серверов: *Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Нет данных*.
Статус Endpoint Sensor	Статус компонента Endpoint Detection and Response component (KATA): *Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Нет данных*.
Создано	Время, когда значок <Имя устройства> был создан. Этот атрибут используется для сравнения различных событий друг с другом.
Имя виртуального или подчиненного Сервера администрирования	Имя виртуального или подчиненного Сервера администрирования. Эта графа доступна только в списках, содержащих устройства с разных Серверов администрирования.
Родительская группа	Название группы администрирования, в которой находится значок <Имя устройства>. Эта графа доступна только в списках, содержащих устройства с разных Серверов администрирования.

Название графы	Значение
Под управлением другого Сервера администрирования	Параметр может принимать одно из следующих значений: • True – если при удаленной установке приложений безопасности на устройство окажется, что устройством управляет другой Сервер администрирования. • False в противном случае.
Номер сборки операционной системы	Номер сборки операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить поиск всех номеров сборки, кроме указанного.
Идентификатор выпуска операционной системы	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.

Статусы устройств, задач и политик

В таблице ниже представлен список значков, отображающихся в дереве консоли и в рабочей области Консоли администрирования рядом с именами устройств, задач и политик. Эти значки характеризуют статус объектов.

Статусы устройств, задач и политик

Значок	Состояние
	Устройство с операционной системой для рабочих станций, обнаруженное в сети и не входящее в состав какой-либо группы администрирования.
	Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, со статусом *OK*.
	Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, со статусом *Предупреждение*.
	Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, со статусом *Критический*.
	Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, соединение которого с Сервером администрирования потеряно.
	Устройство с операционной системой для серверов, обнаруженное в сети и не входящий в состав какой-либо группы администрирования.
	Устройство с операционной системой для серверов, входящее в состав группы администрирования, со статусом *OK*.
	Устройство с операционной системой для серверов, входящее в состав группы администрирования, со статусом *Предупреждение*.
	Устройство с операционной системой для серверов, входящее в состав группы администрирования, со статусом *Критический*.
	Устройство с операционной системой для серверов, входящее в состав группы администрирования, соединение которого с Сервером администрирования потеряно.
	Мобильное устройство, обнаруженное в сети и не входящее в состав какой-либо группы администрирования.
	Мобильное устройство, входящее в состав группы администрирования, со статусом *OK*.
	Мобильное устройство, входящее в состав группы администрирования, со статусом *Предупреждение*.
	Мобильное устройство, входящее в состав группы администрирования, со статусом *Критический*.
	Мобильное устройство, входящее в состав группы администрирования, соединение которого с Сервером администрирования потеряно.

	Устройство с защитой на уровне UEFI, обнаруженное в сети и не входящее в состав какой-либо группы администрирования. Устройство с защитой на уровне UEFI в сети.
	Устройство с защитой на уровне UEFI, обнаруженное в сети и не входящее в состав какой-либо группы администрирования. Устройство с защитой на уровне UEFI не в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом *OK*. Устройство с защитой на уровне UEFI в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом *OK*. Устройство с защитой на уровне UEFI не в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом *Предупреждение*. Устройство с защитой на уровне UEFI в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом *Предупреждение*. Устройство с защитой на уровне UEFI не в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом *Критический*. Устройство с защитой на уровне UEFI в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом *Критический*. Устройство с защитой на уровне UEFI не в сети.
	Активная политика.
	Неактивная политика.
	Активная политика, унаследованная от группы, созданной на главном Сервере администрирования.
	Активная политика, унаследованная от группы верхнего уровня иерархии.
	Задача (групповая, Сервера администрирования или для наборов устройств) в состоянии *Ожидает выполнения* или *Завершена успешно*.
	Задача (групповая, Сервера администрирования или для наборов устройств) в состоянии *Выполняется*.
	Задача (групповая, Сервера администрирования или для наборов устройств) в состоянии *Сбой*.
	Задача, унаследованная от группы, созданной на главном Сервере администрирования.
	Задача, унаследованная от группы верхнего уровня иерархии.

Значки статусов файлов в Консоли администрирования

Для упрощения работы с файлами в Консоли администрирования Kaspersky Security Center рядом с именами файлов отображаются значки (см. таблицу ниже). Значки сигнализируют о статусах, присвоенных файлам управляемыми приложениями "Лаборатории Касперского" на клиентских устройствах. Значки отображаются в рабочей области папок **Карантин**, **Резервное хранилище** и **Активные угрозы**.

Статусы присваиваются объектам приложением Kaspersky Endpoint Security, установленным на клиентском устройстве, на котором находится объект.

Соответствие значков статусам файлов

Значок	Состояние
	Файл со статусом *Заражен*.
	Файл со статусом *Предупреждение* или *Возможно зараженный*.
	Файл со статусом *Добавлено пользователем*.
	Файл со статусом *Ложное срабатывание*.

	Файл со статусом *Вылечен*.
	Файл со статусом *Удален*.
	Файл в папке **Карантин** со статусом *Не заражен, Защищен паролем* или *Необходимо отправить в "Лабораторию Касперского"*. Если рядом со значком нет описания статуса, это означает, что управляемое приложение "Лаборатории Касперского" на клиентском устройстве передало Kaspersky Security Center неизвестный статус.
	Файл в папке **Резервное хранилище** со статусом *Не заражен, Защищен паролем* или *Необходимо отправить в "Лабораторию Касперского"*. Если рядом со значком нет описания статуса, это означает, что управляемое приложение "Лаборатории Касперского" на клиентском устройстве передало Kaspersky Security Center неизвестный статус.
	Файл в папке **Активные угрозы** со статусом *Не заражен, Защищен паролем* или *Необходимо отправить в "Лабораторию Касперского"*. Если рядом со значком нет описания статуса, это означает, что управляемое приложение "Лаборатории Касперского" на клиентском устройстве передало Kaspersky Security Center неизвестный статус.

Поиск и экспорт данных

В этом разделе содержится информация о способах поиска данных и об экспорте данных.

Поиск устройств

Kaspersky Security Center позволяет искать устройства на основании заданных критериев. Результаты поиска можно сохранить в текстовом файле.

Функция поиска позволяет находить следующие устройства:

- клиентские устройства в группах администрирования Сервера администрирования и его подчиненных Серверов;
- нераспределенные устройства под управлением Сервера администрирования и его подчиненных Серверов.

Чтобы искать клиентские устройства, входящие в группу администрирования:

1. В дереве консоли выберите папку группы администрирования.
2. В контекстном меню папки группы администрирования выберите пункт **Поиск**.
3. На вкладках окна **Поиск** укажите критерии, по которым нужно выполнить поиск устройств, и нажмите на кнопку **Найти**.

В результате устройства, соответствующие заданным критериям поиска, отобразятся в таблице в нижней части окна **Поиск**.

Чтобы искать нераспределенные устройства:

1. В дереве консоли выберите папку **Нераспределенные устройства**.
2. В контекстном меню папки **Нераспределенные устройства** выберите пункт **Поиск**.
3. На вкладках окна **Поиск** укажите критерии, по которым нужно выполнить поиск устройств, и нажмите на кнопку **Найти**.

В результате устройства, соответствующие заданным критериям поиска, отобразятся в таблице в нижней части окна **Поиск**.

Чтобы искать устройства независимо от того, входят они в состав групп администрирования или нет:

1. В дереве консоли выберите узел **Сервер администрирования**.
2. В контекстном меню узла Сервера администрирования выберите пункт **Поиск**.
3. На вкладках окна **Поиск** укажите критерии, по которым нужно выполнить поиск устройств, и нажмите на кнопку **Найти**.

В результате устройства, соответствующие заданным критериям поиска, отобразятся в таблице в нижней части окна **Поиск**.

В окне **Поиск** вы можете также искать группы администрирования и подчиненные Серверы администрирования с помощью раскрывающегося списка в правом верхнем углу окна. Поиск групп администрирования и подчиненных Серверов администрирования недоступен при открытии окна **Поиск** из папки **Нераспределенные устройства**.

Для поиска устройств вы можете использовать в полях ввода окна **Поиск** регулярные выражения.

Полнотекстовый поиск в окне **Поиск** доступен:

- на вкладке **Сеть** в поле **Описание**;
- на вкладке **Оборудование** в полях **Устройство**, **Поставщик** и **Описание**.

Параметры поиска устройств

Ниже представлены описания параметров поиска управляемых устройств. Результаты поиска отображаются в таблице в нижней части окна.

Сеть

На вкладке **Сеть** можно настроить критерии поиска устройств на основании их сетевых данных:

- **Имя устройства или IP-адрес**

  Имя устройства в сети Windows (NetBIOS-имя) или IPv4-адрес или IPv6-адрес.

- **Windows-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**. Только клиентские устройства, управляемые другими Серверами администрирования, будут включены в выборку.
  - **Нет**. Только клиентские устройства, управляемые этим же Сервером администрирования, будут включены в выборку.
  - **Значение не выбрано**. Критерий не применяется.

Теги

На вкладке **Теги** можно настроить поиск устройств 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.

- **Тег должен присутствовать**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых есть выбранный тег. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

  По умолчанию выбран этот вариант.

- **Тег должен отсутствовать**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых нет выбранного тега. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

Active Directory

На вкладке **Active Directory** можно указать, что устройства следует искать в подразделении (OU) или группе Active Directory. Также можно включить в выборку устройства из всех дочерних подразделений указанного подразделения Active Directory. Чтобы выбрать устройства, укажите следующие параметры:

- **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 домена.

  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.

Сетевая активность

На вкладке **Сетевая активность** можно указать критерии поиска устройств на основании их сетевой активности:

- **Это устройство 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.

Приложение

На вкладке **Приложение** можно указать критерии поиска устройств на основании выбранного управляемого приложения:

- **Название приложения**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске по наименованию приложения "Лаборатории Касперского".

  В списке представлены названия только тех приложений, для которых на рабочем месте администратора установлены плагины управления.

Если приложение не выбрано, то критерий не применяется.

- **Версия приложения**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по номеру версии приложения "Лаборатории Касперского".

  Если номер версии не указан, то критерий не применяется.

- **Название критического обновления**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по установленному для приложения наименованию или номеру пакета обновления.

  Если поле не заполнено, то критерий не применяется.

- **Последнее обновление модулей приложения**

  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 Kaspersky Security Center**

  В раскрывающемся списке можно включить в состав выборки устройства, которые находятся под управлением Kaspersky Security Center:

  - **Да**. Приложение включает в выборку устройства, которые находятся под управлением Kaspersky Security Center.
  - **Нет**. Приложение включает в выборку устройства, которые не находятся под управлением Kaspersky Security Center.
  - **Значение не выбрано**. Критерий не применяется.

- **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.

Операционная система

На вкладке **Операционная система** можно настроить следующие критерии поиска устройств на основании установленной на них операционной системы:

- **Версия операционной системы**

  Если флажок установлен, в списке можно выбрать операционные системы. Устройства, на которых установлены указанные операционные системы, включаются в результаты поиска.

- **Архитектура операционной системы**

  В раскрывающемся списке можно выбрать архитектуру операционной системы, по наличию которой к устройству применяется правило перемещения (**Нет данных**, **x86**, **AMD64** или **IA64**). По умолчанию в списке не выбран ни один вариант, архитектура операционной системы не задана.

- **Версия пакета обновления операционной системы**

  В поле можно указать версию пакета установленной операционной системы (в формате *X.Y*), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

- **Номер сборки операционной системы**

  > Этот параметр применим только для операционных систем Windows.

  Номер сборки операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить поиск всех номеров сборки, кроме указанного.

- **Идентификатор выпуска операционной системы**

  > Этот параметр применим только для операционных систем Windows.

  Идентификатор выпуска операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний идентификатор выпуска. Вы также можете настроить поиск всех номеров идентификаторов выпуска, кроме указанного.

Статус устройства

На вкладке **Статус устройства** можно указать критерии поиска устройств по статусу 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.

- **Описание статуса устройства**

  В этом поле можно установить флажки для условий, при соблюдении которых устройству будет присваиваться выбранный статус: *OK, Критический* или *Предупреждение*.

- **Статус устройства определен приложением**

  Раскрывающийся список, в котором можно выбрать значение статуса задачи постоянной защиты. Устройства с указанным статусом постоянной защиты будут включаться в выборку.

Компоненты защиты

На вкладке **Компоненты защиты** можно настроить параметры поиска клиентских устройств 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.

- **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.

- **Всего обнаружено угроз**

  Если этот параметр включен, поиск клиентских устройств выполняется по количеству найденных вирусов. В полях ввода можно задать нижнее и верхнее значения количества найденных вирусов.

  По умолчанию параметр выключен.

Реестр приложений

На вкладке **Реестр приложений** можно настроить параметры поиска устройств 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.

Иерархия Серверов администрирования

На вкладке **Иерархия Серверов администрирования**, установите флажок **Включая данные с подчиненных Серверов до уровня**, если вы хотите, чтобы информация, хранящаяся на подчиненных Серверах администрирования, учитывалась при поиске устройств, а в поле ввода можно указать уровень вложенности подчиненного Сервера администрирования, с которого учитывается информация при поиске устройств. По умолчанию флажок снят.

Виртуальные машины

На вкладке **Виртуальные машины** можно настроить параметры поиска 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 следующие элементы:

  - **Неважно**.
  - **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:

  - **Неважно**.
  - **Нет**. Искомые устройства не должны являться частью Virtual Desktop Infrastructure.
  - **Да**. Искомые устройства должны являться частью Virtual Desktop Infrastructure (VDI).

Оборудование

На вкладке **Оборудование** можно настроить поиск клиентских устройств по установленному на них оборудованию:

- **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.

- **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.

- **Инвентарный номер**

  Оборудование с инвентарным номером, указанным в поле, будет включено в выборку.

- **Частота процессора (МГц)**

  Диапазон частот процессора. Устройства с процессорами, соответствующими диапазону частот в полях ввода (включительно), будут включены в состав выборки.

- **Виртуальных ядер процессора**

  Диапазон количества виртуальных ядер процессора. Устройства с процессорами, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем жесткого диска (ГБ)**

  Диапазон значений объема жесткого диска устройства. Устройства с жесткими дисками, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем оперативной памяти (МБ)**

  Диапазон значений объема оперативной памяти устройства. Устройства с оперативной памятью, соответствующей диапазону в полях ввода (включительно), будут включены в состав выборки.

Уязвимости и обновления

На вкладке **Уязвимости и обновления** можно настроить критерии поиска устройств 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.

Пользователи

На вкладке **Пользователи** можно настроить параметры поиска устройств по учетным записям пользователей, выполнявших вход в операционную систему.

- **Последний пользователь, выполнивший вход в систему**

  Если этот параметр включен, при нажатии на кнопку **Обзор** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых последний вход в систему выполнялся указанным пользователем.

- **Пользователь, когда-либо выполнявший вход в систему**

  Если этот параметр включен, при нажатии на кнопку **Обзор** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых указанный пользователь когда-либо выполнял вход в систему.

Проблемы, связанные со статусом управляемых приложений

На вкладке **Проблемы, связанные со статусом управляемых приложений** можно настроить поиск по описаниям статусов устройств от управляемого приложения:

- **Описание статуса устройства**

  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.

Статусы компонентов управляемых приложений

На вкладке **Статусы компонентов управляемых приложений** можно настроить поиск по статусам компонентов управляемых приложений:

- **Статус защиты данных от утечек**

  Поиск устройств по статусу компонента защиты от утечки данных (*Нет данных, Остановлен, Запускается, Приостановлен, Выполняется, Сбой*).

- **Статус защиты для серверов совместной работы**

  Поиск устройств по статусу защиты для серверов совместной работы (*Нет данных*, *Остановлен*, *Запускается, Приостановлен*, *Выполняется*, *Сбой*).

- **Статус антивирусной защиты почтовых серверов**

  Поиск устройств по статусу защиты почтовых серверов (*Нет данных, Остановлен, Запускается, Приостановлен, Выполняется, Сбой*).

- **Статус Endpoint Sensor**

  Поиск устройств по статусу компонента Endpoint Sensor (*Нет данных, Остановлен, Запускается, Приостановлен, Выполняется, Сбой*).

Шифрование

- **Шифрование**

  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*.

Облачные сегменты

На вкладке **Облачные сегменты** можно настроить поиск по принадлежности к облачным сегментам:

- **Устройство находится в облачном сегменте**

  Если флажок установлен, при нажатии на кнопку **Выбрать** можно указать сегмент поиска.

  Если также установлен флажок **Включая вложенные 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:

  - **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.

Компоненты приложения

Этот раздел содержит список компонентов тех приложений, которые имеют соответствующие плагины управления, установленные в Консоли администрирования.

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*, *Остановлено*, *Запускается*, *Приостановлено*, *Выполняется*, *Сбой* или *Не установлено*. Если выбранный компонент приложения, установленный на управляемом устройстве, имеет указанный статус, устройство входит в выборку устройств.

Статусы, отправленные приложениями:

- *Запускается* – компонент в настоящее время находится в процессе инициализации.
- *Выполняется* – компонент включен и работает правильно.
- *Приостановлено* – компонент приостановлен, например, после того, как пользователь приостановил защиту в управляемом приложении.
- *Сбой* – во время выполнения операции компонента произошла ошибка.
- *Остановлено* – компонент отключен и в данный момент не работает.
- *Не установлено* – пользователь не выбрал компонент для установки во время выборочной установки приложения.

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.

Использование масок в строковых переменных

Для строковых переменных допустимо использование масок. Для создания масок вы можете использовать следующие регулярные выражения:

- Знак подстановки (*) – любая строка длиной 0 или более символов.
- Вопросительный знак (?) – один любой символ.
- [<интервал>] – Заменяет один символ из заданного диапазона или множества.

  Например: [0–9] – любая цифра. [abcdef] – один из символов a, b, c, d, e, f.

Использование регулярных выражений в строке поиска

Для поиска отдельных слов и символов вы можете использовать в строке поиска следующие регулярные выражения:

- *. Заменяет последовательность любого количества символов. Например, для поиска слов "Сервер", "Серверный" или "Серверная" в строке поиска нужно ввести выражение `Server*`.
- ?. Заменяет любой один символ. Например, для поиска слов "Окно" или "Окна" в строке поиска нужно ввести выражение `Окн?`.

  > Текст в строке поиска не может начинаться с ?.

- [<интервал>]. Заменяет один символ из заданного диапазона или множества. Например, для поиска любой цифры в строке поиска нужно ввести выражение `[0-9]`. Для поиска одного из символов a, b, c, d, e, f в строке поиска нужно ввести выражение `[abcdef]`.

Для полнотекстового поиска вы можете использовать в строке поиска следующие регулярные выражения:

- Пробел. Результат: все устройства, описания которых содержат любое из перечисленных слов. Например, для поиска фразы, содержащей слово "Подчиненный" или "Виртуальный" (или оба этих слова), в строке поиска нужно ввести выражение `Secondary Virtual`.
- Знак "плюс" (+), AND или &&. При написании перед словом обозначает обязательное наличие слова в тексте. Например, для поиска фразы, содержащей и слово "Подчиненный", и слово "Виртуальный", в строке поиска можно ввести выражения: `+Secondary+Virtual`, `Secondary AND Virtual`, `Secondary && Virtual`.
- OR или ||. При написании между словами обозначает наличие одного или другого слова в тексте. Например, для поиска фразы, содержащей или слово "Подчиненный", или слово "Виртуальный", в строке поиска можно ввести выражения: `Secondary OR Virtual`, `Secondary || Virtual`.
- Знак "минус" (-). При написании перед словом обозначает обязательное отсутствие слова в тексте. Например, для поиска фразы, в которой должно присутствовать слово "Подчиненный", и должно отсутствовать слово "Виртуальный", нужно ввести в строке поиска выражение `+Secondary-Virtual`.
- `"<text fragment>"`. Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте. Например, для поиска фразы, содержащей словосочетание "Подчиненный Сервер", нужно ввести в строке поиска выражение `"Secondary Server"`.

Полнотекстовый поиск доступен в следующих блоках фильтрации:

- в блоке фильтрации списка событий по графам **Событие** и **Описание**;
- в блоке фильтрации учетных записей пользователей по графе **Имя**;
- в блоке фильтрации реестра приложений по графе **Название**, если в блоке **Показывать в списке** выбран критерий фильтрации **без группировки**.

Экспорт списков из диалоговых окон

В диалоговых окнах приложения вы можете экспортировать в текстовые файлы списки объектов.

Экспорт списка объектов возможен для тех разделов диалогового окна, которые содержат кнопку **Экспортировать в файл**.

Параметры задач

В этом разделе перечислены параметры задач Kaspersky Security Center.

Общие параметры задач

Этот раздел содержит описание параметров, которые вы можете просмотреть и настроить для большинства ваших задач. Список доступных параметров зависит от настраиваемой задачи.

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- Параметры перезагрузки операционной системы:

  - **Не перезагружать устройство**

    Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

  - **Перезагрузить устройство**

    В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

  - **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.

- **Принудительное закрытие приложения в заблокированных сессиях через (мин)**

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.

- Параметры расписания задачи:

  > Типы расписаний могут изменяться в зависимости от задачи.

  - **Параметры Запуск по расписанию:**

    - **Каждый N час**

      Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

      По умолчанию задача запускается каждые 6 часов, начиная с текущих системной даты и времени.

    - **Каждые N дней**

      Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются приложением, для которого вы создаете задачу.

      По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

    - **Каждые N минут**

      Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

      По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

  По умолчанию выбран этот вариант.

- **Один раз**

  Задача выполняется один раз, в указанные дату и время (по умолчанию в день создания задачи).

- **Немедленно**

  Задача запускается сразу после сохранения ее параметров.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию указано время 18:00 и не выбраны дни месяца.

  > Обратите внимание, что вы выбираете порядковый номер дня недели в месяце, а не конкретную дату в месяце или номер недели (первая, вторая неделя месяца). Например, если вы выберите ячейку **Вт** в строке **Первая**, в этом случае задача будет запускаться каждый первый вторник каждого нового месяца.

  Вы можете выбрать несколько дней недели.

- **При загрузке обновлений в хранилище**

  Эта задача запускается после загрузки обновлений в хранилище. Например, вам может понадобиться это расписание для задачи поиска уязвимостей и требуемых обновлений.

- **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 случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

- Устройства, которым будет назначена задача:

  - **Выбрать устройства, обнаруженные в сети Сервером администрирования**

    В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

    Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

  - **Задать адреса устройств вручную или импортировать из списка**

    Вы можете задавать 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.

  - **Назначить задачу группе администрирования**

    Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

    Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

    Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, так как групповые задачи подчиняются параметрам групп безопасности, к которым они относятся.

- Параметры учетной записи:

  - **Учетная запись по умолчанию**

    Задача будет запускаться под той же учетной записью, под которой было установлено и запущено приложение, выполняющее эту задачу.

    По умолчанию выбран этот вариант.

  - **Задать учетную запись**

    В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.

- **Учетная запись**

  Учетная запись, от имени которой будет запускаться задача.

- **Пароль**

  Пароль учетной записи, от имени которой будет запускаться задача.

> Если Агент администрирования не установлен на вашем целевом устройстве, нужно указать учетную запись, которая будет использоваться на целевом устройстве для доступа к административным ресурсам общего доступа admin$. Указанная вами учетная запись предназначена только для копирования данных на ваше устройство. Если на вашем целевом устройстве установлен Агент администрирования, данные копируются с помощью Агента администрирования и вам не нужно указывать учетную запись при создании задачи.

Параметры, заданные после создания задачи

Вы можете задать следующие параметры только после создания задачи.

- Параметры групповой задачи:

  - **Распределить по подгруппам**

    Этот параметр доступен только в свойствах групповых задач.

    Когда этот параметр включен, область действия задачи включает в себя:

    - группу администрирования, которую вы выбрали при создании задачи;
    - группы администрирования, подчиненные по отношению к выбранной группе администрирования на любом уровне вниз по иерархии групп.

    Если этот параметр выключен, в состав задачи входит только та группа администрирования, которую выбрали при создании задачи.

    По умолчанию параметр включен.

  - **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 **Распределить по подгруппам** включен.

    По умолчанию параметр выключен.

- Дополнительные параметры расписания:

  - **Активировать устройства перед запуском задачи функцией Wake-on-LAN за (мин)**

    Если флажок установлен, операционная система на устройстве будет загружаться за указанное время до начала выполнения задачи. Время, заданное по умолчанию, – 5 минут.

Включите этот параметр, если вы хотите, чтобы задача выполнялась на всех клиентских устройствах из области задач, включая те устройства, которые выключены, когда задача вот-вот начнется.

Если нужно, чтобы устройства автоматически выключались после выполнения задачи, включите параметр **Выключать устройства после выполнения задачи**. Параметр находится в этом же окне.

По умолчанию параметр выключен.

- **Выключать устройства после выполнения задачи**

  Например, вы можете включить этот параметр для задачи установки обновлений, которая устанавливает обновления на клиентские устройства каждую пятницу после рабочего времени, а затем выключает эти устройства на выходные.

  По умолчанию параметр выключен.

- **Остановить, если задача выполняется дольше (мин)**

  По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

  Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

  По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

- Параметры уведомления:

  - Блок **Сохранять информацию о результатах**:

    - **На Сервере 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.

    - **Хранить в журнале событий ОС на Сервере**

      События приложения, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся централизованно в журнале событий Windows операционной системы Сервера администрирования.

      По умолчанию параметр выключен.

    - **Сохранять все события**

      Если выбран этот параметр, в журнал событий записываются все события, связанные с задачей.

- **Сохранять события, связанные с ходом выполнения задачи**

  Если выбран этот параметр, в журнал событий записываются только события, связанные с выполнением задачи.

- **Сохранять только результат выполнения задачи**

  Если выбран этот параметр, в журнал событий записываются только события, связанные с результатами выполнения задачи.

- **Уведомлять администратора о результатах**

  Вы можете выбрать способы, с помощью которых администраторы получают уведомления о результатах выполнения задачи: по электронной почте, по SMS и при запуске исполняемого файла. Чтобы настроить параметры уведомления, перейдите по ссылке **Параметры**.

  По умолчанию отключены все способы уведомлений.

- **Уведомлять только об ошибках**

  Если этот параметр включен, администраторы получают уведомление, только если задача завершается с ошибкой.

  Если этот параметр выключен, администраторы получают уведомление после каждого завершения задачи.

  По умолчанию параметр включен.

- Параметры безопасности

- Параметры области действия задачи

  В зависимости от того, как определяется область действия задачи, присутствуют следующие параметры:

  - **Устройства**

    Если область действия задачи определяется группами администрирования, вы можете просмотреть эту группу. Никакие изменения здесь недоступны. Однако вы можете настроить **Исключения из области действия задачи**.

    Если область действия задачи определяется списком устройств, вы можете изменить этот список, добавив и удалив устройства.

  - **Выборка устройств**

    Вы можете изменить выборку устройств, к которым применяется задача.

  - **Исключения из области действия задачи**

    Вы можете указать группу устройств, к которым не применяется задача. Группы, подлежащие исключению, могут быть только подгруппами группы администрирования, к которой применяется задача.

- **История ревизий**

Параметры задачи загрузки обновлений в хранилище Сервера администрирования

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- **Источники обновлений**

  В качестве источника обновлений для Сервера администрирования 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 Сервер администрирования взаимодействует с серверами обновлений "Лаборатории Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.

    Выбрано по умолчанию.

  - Главный Сервер администрирования

    Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.

  - Локальная или сетевая папка

    Локальная или сетевая папка, которая содержит последние обновления. Сетевая папка может быть FTP-сервером, HTTP-сервером или общим ресурсом SMB. 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".

- **Прочие параметры**

  Принудительно обновить подчиненные Серверы

  Если параметр включен, Сервер администрирования будет запускать задачи получения обновлений на подчиненных Серверах администрирования сразу после получения обновлений. Задачи обновления запускаются с использованием источника обновления, который настроен в свойствах задачи на подчиненных Серверах администрирования.

  Если этот параметр выключен, задачи обновления на подчиненных Серверах администрирования начинаются в соответствии с расписанием.

  По умолчанию параметр выключен.

  Копировать полученные обновления в дополнительные папки

Если флажок установлен, после получения обновлений Сервер администрирования будет копировать обновления в указанные папки. Используйте этот параметр, если хотите управлять вручную обновлениями на вашем устройстве.

Например, вы можете использовать этот параметр в следующей ситуации: сеть организации содержит несколько независимых подсетей и устройства из каждой подсети не имеют доступ к другой подсети. При этом устройства во всех подсетях имеют доступ к общей сетевой папке. В этом случае для Сервера администрирования в одной из подсетей укажите загрузку обновлений с серверов обновлений "Лаборатории Касперского", включите этот параметр и укажите эту сетевую папку. В задаче загрузка обновлений в хранилище для Сервера администрирования укажите эту же сетевую папку в качестве источника обновлений.

Если вы выберете копирование загруженных обновлений в локальную папку, необходимо указать на устройстве папку, которая содержит установленный Сервер администрирования. Путь к папке зависит от операционной системы устройства. Поскольку локальная папка расположена на Сервере администрирования с операционной системой Linux, вам нужно указать POSIX-путь, например, /path/to/dir.

При выборе сетевой папки, расположенной на Сервере администрирования с операционной системой Linux, нужно заранее обеспечить доступ к сетевой папке с устройства, на котором установлен Сервер администрирования, смонтировав папку. Доступ к папке осуществляется с использованием SMB-протокола.

По умолчанию параметр выключен.

Не обновлять устройства и подчиненные Серверы администрирования принудительно до окончания копирования

Если флажок установлен, задачи получения обновлений клиентскими устройствами и подчиненными Серверами администрирования будут запускаться после окончания копирования обновлений из сетевой папки обновлений в дополнительные папки обновлений.

Этот флажок должен быть установлен, если клиентские устройства и подчиненные Серверы администрирования скачивают обновления из дополнительных сетевых папок.

По умолчанию параметр выключен.

Параметры, заданные после создания задачи

Вы можете задать следующие параметры только после создания задачи.

- Раздел **Параметры**, блок **Состав обновлений**

  Загрузить файлы различий

  Этот параметр включает функцию загрузки файлов различий.

  По умолчанию параметр выключен.

- Раздел **Проверка обновлений**

  Выполнять проверку обновлений перед распространением

Если флажок установлен, Сервер администрирования копирует обновления из источника, сохраняет их во временном хранилище и запускает задачу Проверка обновлений, указанную в поле **Задача проверки обновлений**. В случае успешного выполнения этой задачи обновления копируются из временного хранилища в папку общего доступа Сервера администрирования и распространяются на устройства, для которых Сервер администрирования является источником обновлений (запускаются задачи с типом расписания **При загрузке обновлений в хранилище**). Задача загрузки обновлений в хранилище считается завершенной только после завершения задачи *Проверка обновлений*.

По умолчанию параметр выключен.

Задача проверки обновлений

Эта задача проверяет загруженные обновления перед тем как распространить их на все устройства, для которых Сервер администрирования выбран в качестве источника обновлений.

В этом поле можно указать задачу *Проверка обновлений*, которая была создана ранее. Также вы можете создать другую задачу *Проверка обновлений*.

Параметры задачи загрузки обновлений в хранилища точек распространения

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- **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.

  - Главный Сервер администрирования

    Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.

  - Локальная или сетевая папка

    Локальная или сетевая папка, которая содержит последние обновления. Сетевая папка может быть FTP-сервером, HTTP-сервером или общим ресурсом SMB. Если сетевая папка требует проверки подлинности, поддерживается только SMB-протокол. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

    > FTP-сервер, HTTP-сервер или сетевая папка, используемые в качестве источника обновлений, должны содержать структуру папок (с обновлениями), которая соответствует структуре папок, созданной при использовании серверов обновлений "Лаборатории Касперского".

- **Прочие параметры → 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.

Параметры, заданные после создания задачи

Вы можете указать следующие параметры в разделе **Параметры** в блоке **Состав обновлений** только после создания задачи.

Загрузить файлы различий

Этот параметр включает функцию загрузки файлов различий.

По умолчанию параметр выключен.

Параметры задачи поиска уязвимостей и требуемых обновлений.

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- **Поиск уязвимостей и обновлений, перечисленных Microsoft**

  При поиске уязвимостей и обновлений Kaspersky Security Center использует данные о применимых обновлениях Microsoft из источника обновлений Microsoft, доступного в текущий момент.

  Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft и обновлений сторонних приложений.

  По умолчанию параметр включен.

  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 (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 не запрашивает информацию об обновлениях.

- **Поиск уязвимостей и сторонних обновлений, перечисленных "Лабораторией Касперского"**

  Если этот параметр включен, Kaspersky Security Center выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите пути для дополнительного поиска приложений в файловой системе**. Полный список поддерживаемых приложений сторонних производителей контролируется "Лабораторией Касперского".

  Если этот параметр выключен, Kaspersky Security Center не выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних приложений.

  По умолчанию параметр включен.

  - **Укажите пути для дополнительного поиска приложений в файловой системе**

    Папки, в которых Kaspersky Security Center выполняет поиск сторонних приложений, требующих закрытия уязвимостей и установки обновлений. Вы можете использовать системные переменные.

Укажите папки, в которые были установлены приложения. По умолчанию список содержит системные папки, в которые устанавливается большинство приложений.

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать файлы трассировки, даже если запись файлов трассировки выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

  При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

  По умолчанию параметр выключен.

  - **Максимальный размер файлов расширенной диагностики, МБ**

    По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

Параметры задачи установки требуемых обновлений и закрытия уязвимостей

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- **Задайте правила установки обновлений**

  Эти правила применяются при установке обновлений на клиентские устройства. Если правила не указаны, задача не выполняется. Дополнительную информацию о работе с правилами см. в разделе Правила установки обновлений.

- **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.

- **Загружать обновления на устройство, не устанавливая их**

  Если флажок установлен, приложение загружает обновления на устройство, но не устанавливает их автоматически. Затем вы можете вручную установить загруженные обновления.

  Обновления Microsoft загружаются в служебную папку Windows. Обновления сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) загружаются в папку, указанную в поле **Загрузить обновления для**.

  Если этот параметр выключен, обновления автоматически устанавливаются на устройство.

  По умолчанию параметр выключен.

  - **Загрузить обновления для**

    Эта папка используется для загрузки обновлений сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft).

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать файлы трассировки, даже если запись файлов трассировки выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

  При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

  По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

Параметры, заданные после создания задачи

Вы можете задать параметры, перечисленные ниже, только после создания задачи. Полное описание параметров задачи см. в разделе Общие параметры задач.

- **Общие**. В этом разделе отображается общая информация о задаче. Также можно указать, на какие устройства должна применяться задача *Установка требуемых обновлений и закрытие уязвимостей*.

  - **Распределить по подгруппам**

    Этот параметр доступен только в свойствах групповых задач.

    Когда этот параметр включен, область действия задачи включает в себя:

    - группу администрирования, которую вы выбрали при создании задачи;
    - группы администрирования, подчиненные по отношению к выбранной группе администрирования на любом уровне вниз по иерархии групп.

    Если этот параметр выключен, в состав задачи входит только та группа администрирования, которую выбрали при создании задачи.

    По умолчанию параметр включен.

  - **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 **Распределить по подгруппам** включен.

    По умолчанию параметр выключен.

- Обновления для установки

  В разделе **Обновления для установки** вы можете просмотреть список обновлений, которые заданы в задаче. Отображаются только обновления, соответствующие параметрам выбранной задачи.

- Пробная установка обновлений:

  - **Не проверять**. Выберите этот вариант, если вы не хотите выполнять проверочную установку обновлений.

  - **Выполнить проверку на указанных устройствах**. Выберите этот вариант, если вы хотите проверить установку обновлений на определенных устройствах. Нажмите на кнопку **Добавить** и выберите устройства, на которых нужно выполнить проверочную установку обновлений.

- **Выполнить проверку на устройствах в указанной группе**. Выберите этот вариант, если вы хотите проверить установку обновлений на группе устройств. В поле **Задайте тестовую группу** укажите группу устройств, на которых нужно выполнить проверочную установку.

- **Выполнить проверку на указанном проценте устройств**. Выберите этот вариант, если вы хотите выполнить проверку обновлений на части устройств. В поле **Процент тестовых устройств из общего числа устройств** укажите процент устройств, на которых нужно выполнить проверочную установку обновлений.

Глобальный список подсетей

В этом разделе приведена информация о глобальном списке подсетей, которые вы можете использовать в правилах.

Чтобы сохранить информацию о подсетях вашей сети, вы можете настроить глобальный список подсетей для каждого Сервера администрирования. Этот список позволит сопоставить пары {IP-адрес, маска} и физические единицы, такие как офисы филиалов. Вы можете использовать подсети из этого списка в сетевых правилах и параметрах.

Добавление подсети в глобальный список подсетей

Вы можете добавлять подсети и их описание в глобальный список подсетей.

Чтобы добавить подсеть в глобальный список подсетей:

1. В дереве консоли выберите требуемый узел Сервера администрирования.

2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

3. В открывшемся окне **Свойства** в панели **Разделы** выберите раздел **Список глобальных подсетей**.

4. Нажмите на кнопку **Добавить**.

   Откроется окно **Новая подсеть**.

5. Заполните следующие поля:

   - **Общие параметры**

     IP-адрес подсети, которую вы добавляете.

   - **Маска подсети**

     Маска подсети, которую вы добавляете.

   - **Имя**

     Имя подсети. Имя подсети должно быть уникальным для всего глобального списка подсетей. Если вы указали имя подсети, которое уже существует в списке, то ей будет добавлен индекс, например: ~~1, ~~2.

- **Описание**

  Описание может содержать дополнительную информацию, например, о филиале, которому принадлежит эта подсеть. Этот текст возникает везде, где отображается список подсетей, например, в списке правил ограничения трафика.

  Это поле не обязательно для заполнения и может быть пустым.

6. Нажмите на кнопку **OK**.

Подсеть появится в списке подсетей.

Просмотр и изменение свойств подсети в глобальном списке подсетей

Вы можете просматривать и изменять свойства подсетей в глобальном списке подсетей.

Чтобы просмотреть или изменить свойства подсети в глобальном списке подсетей:

1. В дереве консоли выберите требуемый узел Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В открывшемся окне **Свойства** в панели **Разделы** выберите раздел **Список глобальных подсетей**.
4. В списке выберите требуемую подсеть.
5. Нажмите на кнопку **Свойства**.

   Откроется окно **Новая подсеть**.
6. Если необходимо, измените параметры подсети.
7. Нажмите на кнопку **OK**.

Если вы сделали изменения, то они будут сохранены.

Использование Агента администрирования для Windows, Linux и macOS: сравнение

Использование Агента администрирования зависит от операционной системы устройства. Свойства политики Агента администрирования и инсталляционного пакета зависят от операционной системы. В таблице ниже сравниваются возможности и сценарии использования Агента администрирования, доступные для операционных систем Windows, macOS и Linux.

Сравнение функций Агента администрирования

Функция Агента администрирования	Windows	Linux	macOS
Установка			
Автоматическое создание инсталляционного пакета Агента администрирования, после установки Kaspersky Security Center	✓	–	–

Функция Агента администрирования	Windows	Linux	macOS
Принудительная установка с помощью соответствующих параметров задачи удаленной установки приложения Kaspersky Security Center	✓	✓	✓
Установка приложений с помощью рассылки пользователям устройств ссылок на автономные пакеты, сформированные Kaspersky Security Center	✓	✓	✓
Установка путем клонирования образа жесткого диска с операционной системой и установленным Агентом администрирования, средствами, предоставляемыми Kaspersky Security Center для работы с образами дисков	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	–	–
Установка методом клонирования образа жесткого диска администратора с операционной системой и Агентом администрирования сторонними средствами	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓	✓
Установка приложений с помощью сторонних средств удаленной установки приложений	✓	✓	✓
Установка вручную с помощью запуска инсталляторов приложений на устройствах	✓	✓	✓
Установка Агента администрирования в тихом режиме	✓	✓	✓
Подключение клиентского устройства к Серверу администрирования вручную	✓	✓	✓
Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center	✓	✓	–
Автоматическое распространение ключа	✓	✓	✓
Принудительная синхронизация	✓	✓	✓ За исключением push-сервера
Точка распространения			
Использование точки распространения	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓	✓

Функция Агента администрирования	Windows	Linux	macOS
Расчет количества и конфигурации точек распространения	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓ Без использования Network Location Awareness (NLA).	✓ Без использования Network Location Awareness (NLA).
Опрос сети	✓ • Опрос сети Windows • Опрос IP-диапазонов • Опрос контроллеров домена (Microsoft Active Directory) Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓ • Опрос IP-диапазонов • Опрос Zeroconf • Опрос контроллеров домена (Microsoft Active Directory, Samba 4 Active Directory)	—
Запуск службы прокси-сервер KSN на стороне точки распространения	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓	—
Загрузка обновлений через серверы обновлений "Лаборатории Касперского" в хранилища точек распространения, которые распространяют обновления на управляемые устройства	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓	— Если устройства с операционной системой Linux или macOS находятся в области действия задачи Загрузка обновлений в хранилища точек распространения, задача завершится со статусом Сбой, даже если она успешно завершилась на всех устройствах с операционной системой Windows.
Принудительная установка приложений	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	С ограничением: невозможно выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой Linux.	С ограничением: невозможно выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой macOS.
Использовать в качестве push-сервера	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓	—
Работа с приложениями сторонних производителей			
Удаленная установка приложений на устройства	✓	—	✓ Подробнее см. в статье Удаленная установка приложений на устройства с операционной системой macOS.
Обновления программного обеспечения	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	—	—
Настройка обновлений операционной системы в политике Агента администрирования	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	—	—
Просмотр информации об уязвимостях в приложениях	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	—	—

Функция Агента администрирования	Windows	Linux	macOS
Поиск уязвимостей в приложениях	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	—	—
Инвентаризация программного обеспечения, установленного на устройствах	✓	✓	—
Виртуальные машины			
Установка Агента администрирования на виртуальные машины	✓	✓	✓
Оптимизация параметров для VDI	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓	✓
Поддержка динамических виртуальных машин	✓ Ограничение: не поддерживается Агентом администрирования для Microsoft Windows на Arm.	✓	✓
Другое			
Аудит действий на удаленном клиентском устройстве с помощью совместного доступа к рабочему столу Windows	✓	—	—
Мониторинг состояния антивирусной защиты	✓	✓	✓
Управление перезагрузкой устройств	✓	—	—
Поддержка отката файловой системы	✓	✓	✓
Использование Агента администрирования в качестве шлюза соединений	✓	✓	✓
Менеджер соединений	✓	✓	✓
Переключение Агента администрирования с одного Сервера администрирования на другой (автоматически по сетевому местоположению)	✓	—	✓
Проверка соединения клиентского устройства с Сервером администрирования. Утилита klnagchk	✓	✓	✓
Удаленное подключение к рабочему столу клиентского устройства	✓	—	✓ С помощью системы Virtual Network Computing (VNC).
Загрузка автономного инсталляционного пакета с помощью мастера переноса данных	✓	✓	✓

Функция Агента администрирования	Windows	Linux	macOS
Опрос Zeroconf	—	✓	—
Просмотр информации об аппаратном обеспечении клиентских устройств	✓	✓ Информация об аппаратном обеспечении устройств с операционной системой Linux передается на Сервер администрирования Агентом администрирования, который установлен на этих устройствах, и ограничивается информацией, указанной в описании параметров управляемого устройства для Консоли администрирования и Kaspersky Security Center Web Console.	✓ Информация об аппаратном обеспечении устройств с операционной системой macOS передается на Сервер администрирования Агентом администрирования, который установлен на этих устройствах, и ограничивается информацией, указанной в описании параметров управляемого устройства для Консоли администрирования и Kaspersky Security Center Web Console.

Kaspersky Security Center Web Console

Kaspersky Security Center Web Console (далее также Kaspersky Security Center Web Console) представляет собой веб-приложение, предназначенное для контроля состояния системы безопасности сети, находящейся под защитой приложений "Лаборатории Касперского".

С помощью приложения вы можете выполнять следующие действия:

- контролировать состояние системы безопасности вашей организации;
- устанавливать приложения "Лаборатории Касперского" на устройства вашей сети и управлять установленными приложениями;
- управлять политиками, сформированными для устройств вашей сети;
- управлять учетными записями пользователей;
- управлять задачами приложений, установленных на устройствах сети;
- просматривать отчеты о состоянии системы безопасности;
- управлять рассылкой отчетов заинтересованным лицам: системным администраторам и другим IT-специалистам.

Для информации о требованиях к аппаратному и программному обеспечению см. требования для Web Console.

Kaspersky Security Center Web Console предоставляет веб-интерфейс, который обеспечивает ваше взаимодействие с Сервером администрирования с помощью браузера. Сервер администрирования – это приложение, которое служит для управления приложениями "Лаборатории Касперского", установленными на устройства вашей сети. Сервер администрирования связывается с устройствами вашей сети через защищенные (SSL) каналы связи. Когда вы с помощью браузера подключаетесь к Kaspersky Security Center Web Console, браузер устанавливает с Сервером Kaspersky Security Center Web Console защищенное (HTTPS) соединение.

Kaspersky Security Center Web Console работает следующим образом:

1. Вы подключаетесь к Kaspersky Security Center Web Console с помощью браузера, в окне которого отображаются страницы веб-портала приложения.
2. С помощью элементов управления веб-портала вы выбираете команду, которую хотите выполнить. Kaspersky Security Center Web Console выполняет следующие действия:
   - Если вы выбрали команду, связанную с получением информации (например, просмотр списка устройств), Kaspersky Security Center Web Console формирует запрос на получение информации к Серверу администрирования, затем получает от него необходимые данные и передает их браузеру в удобном для отображения виде.
   - Если вы выбрали команду управления (например, удаленная установка приложения), Kaspersky Security Center Web Console получает команду от браузера и передает ее Серверу администрирования. Затем приложение получает результат выполнения команды от Сервера администрирования и передает результат браузеру в удобном для отображения виде.

Kaspersky Security Center Web Console представляет собой многоязыковое приложение. Вы можете изменить язык интерфейса в любое время без повторного открытия приложения. Если вы устанавливаете Kaspersky Security Center Web Console совместно с Kaspersky Security Center, Kaspersky Security Center Web Console имеет тот же язык интерфейса что и установочный файл. Если вы устанавливаете только Kaspersky Security Center Web Console, приложение имеет тот же язык что и операционная система. Если Kaspersky Security Center Web Console не поддерживает язык установочного файла или операционной системы, по умолчанию устанавливается английский язык.

Управление мобильными устройствами не поддерживается в Kaspersky Security Center Web Console. Однако если вы добавили мобильные устройства в группу администрирования в Консоли администрирования, эти устройства также отображаются в Kaspersky Security Center Web Console.

Схема развертывания Сервера администрирования Kaspersky Security Center и Kaspersky Security Center Web Console

На следующем рисунке приведена схема развертывания Сервера администрирования Kaspersky Security Center и Kaspersky Security Center Web Console.

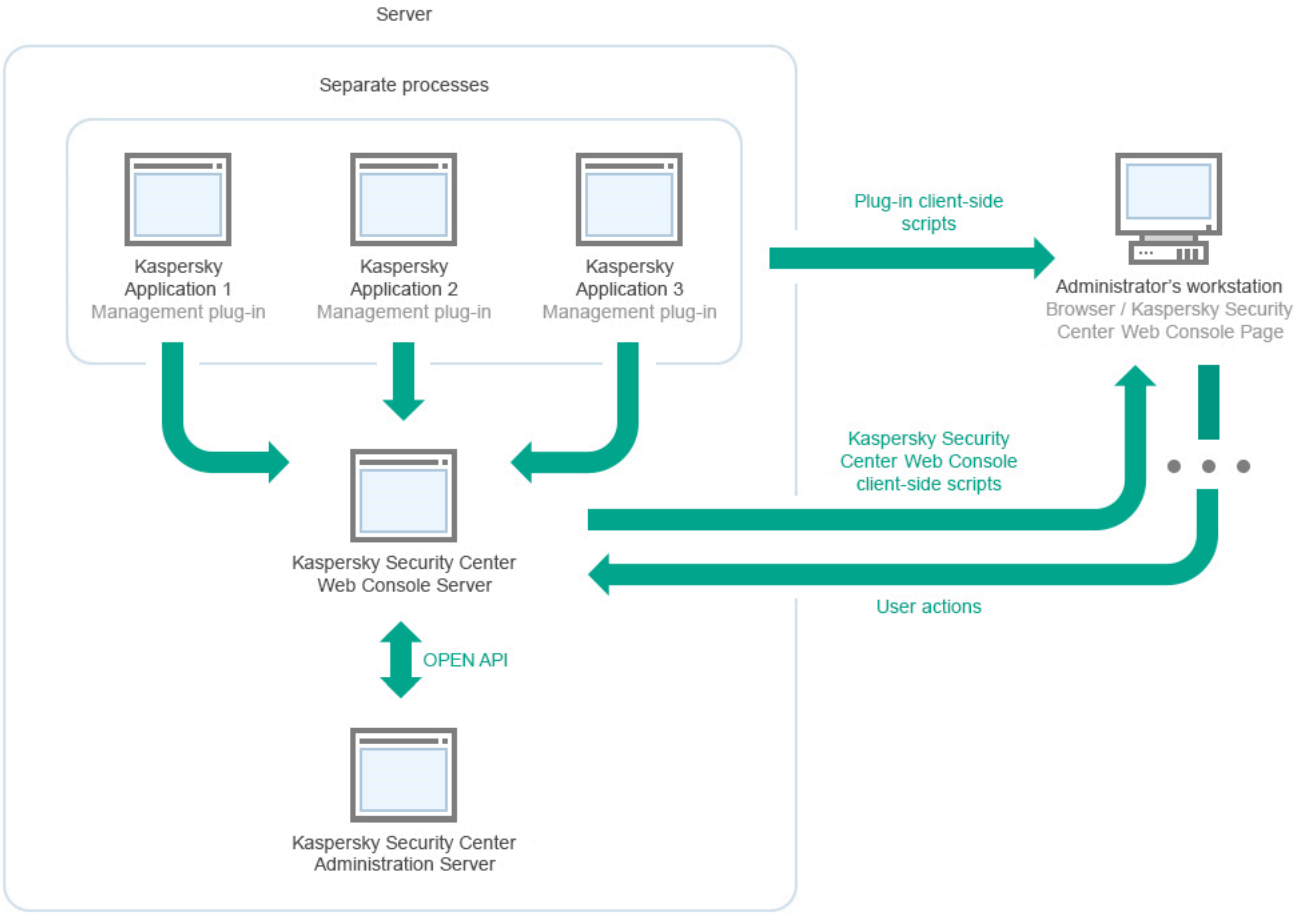


Схема развертывания Сервера администрирования Kaspersky Security Center и Kaspersky Security Center Web Console

Развертывание плагинов управления приложениями "Лаборатории Касперского", установленных на защищаемых устройствах (отдельный плагин для каждого приложения), происходит одновременно с развертыванием Сервера Kaspersky Security Center Web Console.

Как администратор, вы имеете доступ к Kaspersky Security Center Web Console через браузер на вашей рабочей станции.

Когда вы выполняете определенные действия в Kaspersky Security Center Web Console, Сервер Kaspersky Security Center Web Console взаимодействует с Сервером администрирования Kaspersky Security Center по OpenAPI. Сервер Kaspersky Security Center Web Console запрашивает необходимые данные у Сервера администрирования Kaspersky Security Center и отображает результаты ваших действий в Kaspersky Security Center Web Console.

Порты, используемые приложением Kaspersky Security Center Web Console

В таблице ниже перечислены порты, которые должны быть открыты на устройстве, на котором установлен Сервер Kaspersky Security Center Web Console (далее также просто Kaspersky Security Center Web Console).

Порты, используемые приложением Kaspersky Security Center Web Console

Номер порта	Имя службы	Протокол	Назначение порта	Область
2001	Kaspersky Security Center Product Plugins Server	HTTPS	API-порт, который используется процессами плагина управления для приема запросов от службы Kaspersky Security Center Web Console Management Service	Запуск процессов node.exe плагинов управления
1329, 2003	Kaspersky Security Center Web Console Management Service	HTTPS	API-порты, которые используются для получения запросов от службы Kaspersky Security Center Web Console Management Service, работающей на том же устройстве.	Обновление компонентов Kaspersky Security Center Web Console.
2005	Kaspersky Security Center Web Console	HTTPS	API-порт, который используется для получения запросов от службы "Kaspersky Security Center Web Console Management Service", работающей на том же устройстве.	Запуск установки Kaspersky Security Center Web Console
3333	Kaspersky OSMP KAS Service	HTTPS	Порт конечной точки авторизации OAuth2.0	Identity and Access Manager
4004	Kaspersky OSMP Facade Service	HTTPS	Порт провайдера идентификации OAuth2.0	Identity and Access Manager
4444	Kaspersky OSMP KAS Service	HTTPS	Порт конечной точки самоанализа токена OAuth2.0	Identity and Access Manager
8200	—	HTTP	API-порт, который используется для генерации сертификатов с помощью HashiCorp Vault (подробнее см. на сайте HashiCorp Vault).	Установка Kaspersky Security Center Web Console и обновление компонентов Kaspersky Security Center Web Console.
4150, 4151, 4152	Kaspersky Security Center Web Console Message Queue	HTTPS	API-порты Message Broker, которые используются для связи между Kaspersky Security Center Web Console и плагинами управления.	Взаимодействие между Kaspersky Security Center Web Console и плагинов управления

В таблице ниже перечислены порты, которые необязательно открывать на устройстве, на котором установлен Сервер Kaspersky Security Center Web Console. Однако Kaspersky Security Center Web Console использует эти порты для Identity and Access Manager.

Номер порта	Имя службы	Протокол	Назначение порта	Область
4445	Kaspersky OSMP KAS Service	HTTPS	Основной порт Identity and Access Manager, который получает конфигурацию от Kaspersky Security Center Web Console для порта конечной точки авторизации OAuth2.0 (подробнее о OAuth 2.0 см. веб-сайт OAuth)	Identity and Access Manager
2444	Kaspersky OSMP Facade Service	HTTPS	Порт для настройки Identity and Access Manager	Identity and Access Manager
2445	Kaspersky OSMP Facade Service	HTTPS	Порт для подключения службы Kaspersky OSMP KAS Service к службе Kaspersky OSMP Facade Service	Identity and Access Manager

Интерфейс Kaspersky Security Center Web Console

Управление Kaspersky Security Center осуществляется через интерфейс Kaspersky Security Center Web Console.

Окно Kaspersky Security Center Web Console содержит следующие элементы:

- главное меню в левой части окна;
- рабочая область в правой части окна.

Главное меню

Главное меню содержит следующие разделы:

- **Сервер администрирования**. Отображает имя Сервера администрирования, к которому вы сейчас подключены. Нажмите на значок параметров (), чтобы открыть свойства Сервера администрирования.
- **Мониторинг и отчеты**. Предоставляет сведения об инфраструктуре вашей сети, статусе защиты, а также статистику.
- **Активы (Устройства)**. Содержит инструменты для активов, 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 различные параметры, включая лицензирование приложений, просмотр и управление зашифрованными жесткими дисками и событиями шифрования, а также 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. Этот раздел содержит мастер первоначальной настройки и мастер развертывания защиты.
- **Marketplace**. Содержит информацию о бизнес-решениях "Лаборатории Касперского", позволяет выбрать нужные вам и перейти к приобретению этих решений на сайте "Лаборатории Касперского".

- **Параметры**. Позволяет создавать резервную копию данных текущего состояния веб-плагина, чтобы впоследствии можно было восстановить сохраненное состояние. Содержит личные параметры, связанные с внешним видом интерфейса, такие как язык интерфейса или тема.

- **Меню вашей учетной записи**. Содержит ссылку на справку Kaspersky Security Center. Также вы можете выйти из Kaspersky Security Center и просмотреть версию Kaspersky Security Center Web Console и список установленных веб-плагинов управления.

Рабочая область

В рабочей области отображается выбранная вами информация для просмотра в разделах окон интерфейса Kaspersky Security Center Web Console. Она также содержит элементы управления, которые можно использовать для настройки отображения информации.

Закрепление и отмена закрепления разделов главного меню

Вы можете закрепить разделы Kaspersky Security Center Web Console, чтобы добавить их в избранное и быстро получить к ним доступ из раздела **Закрепленное** в главном меню.

> Если закрепленных элементов нет, раздел **Закрепленное** не отображается в главном меню.

Вы можете закрепить разделы, в которых отображаются только страницы. Например, если вы перейдете в раздел **Активы (Устройства)** → **Управляемые устройства**, откроется страница с таблицей устройств, что означает, что вы можете закрепить раздел **Управляемые устройства**. Если после выбора раздела в главном меню отображается окно или элемент не отображается, то закрепить такой раздел невозможно.

Чтобы закрепить раздел:

1. В главном меню наведите курсор мыши на раздел, который вы хотите закрепить.

   Отображается значок булавки (📌).

2. Нажмите на значок булавки (📌).

   Раздел закреплен и отображается в разделе **Закрепленное**.

Вы также можете удалить элементы из избранных, отменив их закрепление.

Чтобы отменить закрепление раздела:

1. В главном окне приложения перейдите в раздел **Закрепленное**.

2. Наведите курсор мыши на раздел, для которого вы хотите отменить закрепление и нажмите на значок отмены закрепления (📌).

   Раздел удален из избранных.

Сценарий: установка и первоначальная настройка Kaspersky Security Center Web Console

В этом разделе описана установка Сервера администрирования Kaspersky Security Center и Kaspersky Security Center Web Console, первоначальная настройка Сервера администрирования с помощью мастера первоначальной настройки, а также установка приложений "Лаборатории Касперского" на управляемые устройства с помощью мастера развертывания защиты.

Установка и первоначальная настройка Kaspersky Security Center Web Console состоит из следующих этапов:

1. **Установка системы управления базами данных (СУБД)**

   Установите СУБД, используемую Kaspersky Security Center, или используйте существующую СУБД.

   Подробнее о том как установить выбранную СУБД, см. в документации к этой СУБД.

2. **Установка Сервера администрирования, Консоли администрирования и Агента администрирования**

   Вместе с Сервером администрирования устанавливаются также Консоль администрирования и серверная версия Агента администрирования.

   Во время установки Сервера администрирования Kaspersky Security Center можно указать, требуется ли устанавливать на это же устройство Kaspersky Security Center Web Console. Если вы решили установить оба компонента на одно устройство, то вам не потребуется устанавливать отдельно приложение Kaspersky Security Center Web Console, так как оно будет установлено автоматически. Если вы хотите установить Kaspersky Security Center Web Console на другое устройство, то после установки Сервера администрирования Kaspersky Security Center перейдите к установке Kaspersky Security Center Web Console.

3. **Установка Kaspersky Security Center Web Console**

   Если вы не выбрали на предыдущем шаге установку Kaspersky Security Center Web Console совместно с Сервером администрирования Kaspersky Security Center, установите Kaspersky Security Center Web Console на другом устройстве. Kaspersky Security Center Web Console можно установить отличном устройстве от устройства, на котором установлен Сервер администрирования.

4. **Выполнение первоначальной настройки**

   После завершения установки Сервера администрирования при первом подключении к Серверу администрирования автоматически запускается Мастер первоначальной настройки. Выполните первоначальную настройку Сервера администрирования в соответствии с вашими требованиями. На этапе первоначальной настройки мастер создает необходимые для развертывания защиты политики и задачи с параметрами по умолчанию. Эти параметры могут оказаться неоптимальными для нужд вашей организации. При необходимости вы можете изменить параметры политик и задач.

5. **Лицензирование Kaspersky Security Center (если требуется)**

   Kaspersky Security Center с поддержкой базовой функциональности Консоли администрирования не требует лицензии. Вам необходима коммерческая лицензия, если вы хотите использовать одну или несколько дополнительных возможностей приложения, включая Системное администрирование, Управление мобильными устройствами и интеграции с SIEM-системами. Вы можете добавить файл ключа или код активации для этих возможностей на соответствующем шаге мастера первоначальной настройки или вручную.

6. **Обнаружение сетевых устройств**

   Этот этап обрабатывается мастером первоначальной настройки. Обнаружение устройств можно также выполнить вручную. В результате Сервер администрирования Kaspersky Security Center получает адреса и имена всех устройств, зарегистрированных в сети. В дальнейшем вы можете с помощью Kaspersky Security Center устанавливать приложения "Лаборатории Касперского" и других производителей на обнаруженные устройства. Kaspersky Security Center запускает обнаружение устройств регулярно, поэтому, если в сети появятся новые устройства, они будут обнаружены автоматически.

7. **Объединение устройств в группы администрирования**

   Этот этап обрабатывается мастером первоначальной настройки, но вы также можете переместить обнаруженные устройства в группы администрирования вручную.

8. **Установка Агента администрирования и приложений безопасности на устройства в сети**

   Развертывание защиты в сети организации подразумевает установку Агента администрирования и приложений безопасности (например, Kaspersky Endpoint Security для Windows) на устройства, найденные Сервером администрирования в процессе обнаружения устройств.

   Чтобы выполнить удаленную установку приложений, запустите мастер развертывания защиты.

   Приложения безопасности защищают устройства от вирусов и других приложений, представляющих угрозу. Агент администрирования обеспечивает связь устройства с Сервером администрирования. Параметры Агента администрирования автоматически настраиваются по умолчанию.

   Перед тем как установить Агент администрирования и приложения безопасности на устройства в сети, убедитесь, что эти устройства доступны (включены).

9. **Распространение лицензионных ключей на клиентские устройства**

   Распространите лицензионные ключи на клиентские устройства, чтобы активировать управляемые приложения безопасности на этих устройствах.

10. **Установка Kaspersky Security для мобильных устройств (необязательно)**

    Если вы планируете управлять корпоративными мобильными устройствами, см. справку Kaspersky Security для мобильных устройств информацию о развертывании Kaspersky Endpoint Security для Android.

11. **Настройка политик приложений "Лаборатории Касперского"**

    Чтобы на различных устройствах были применены разные параметры приложений, можно использовать управление безопасностью устройств или управление безопасностью, ориентированное на пользователей. Управление безопасностью устройств реализуется с помощью политик и задач. Задачи могут выполняться только на устройствах, которые соответствуют определенным условиям. Для создания условий отбора устройств используются выборки устройств и теги.

12. **Мониторинг состояния защиты сети**

    Вы можете организовывать мониторинг сети с помощью виджетов на информационной панели, формировать отчеты о приложениях "Лаборатории Касперского", настраивать и просматривать выборки событий, полученные от приложений на управляемых устройствах, и просматривать список уведомлений.

Установка

В этом разделе описана установка Kaspersky Security Center и Kaspersky Security Center Web Console.

Установка Kaspersky Security Center (Стандартная установка)

В этом разделе описана установка Kaspersky Security Center. Сначала необходимо установить систему управления базами данных.

Чтобы установить Kaspersky Security Center:

1. Запустите исполняемый файл ksc_<номер сборки>_full_<язык локализации>.exe под учетной записью с правами администратора.
2. В открывшемся окне выбора приложений выберите пункт **Установить Kaspersky Security Center**.

   Откроется окно мастера установки Сервера администрирования Kaspersky Security Center.
3. Начав с окна приветствия, пройдите шаги мастера, нажимая на кнопку **Далее**.
4. Установите Microsoft .NET Framework, если он не установлен.
5. Примите условия Лицензионного соглашения и Политики конфиденциальности.
6. Выберите тип установки. Для ознакомительных целей рекомендуется оставить указанный по умолчанию тип – **Стандартная**.
7. Если требуется установить Kaspersky Security Center Web Console на то же устройство, что и Kaspersky Security Center, установите флажок **Установить Kaspersky Security Center Web Console**.

   Если этот флажок не установлен, вы можете установить Kaspersky Security Center Web Console отдельно на это же или другое устройство.
8. Укажите размер сети. Для ознакомительных целей рекомендуется оставить указанное по умолчанию значение – **Менее 100 устройств в сети**.
9. Выберите тип установленного ранее сервера базы данных.
10. Укажите параметры подключения к установленному ранее серверу баз данных.
11. Укажите параметры аутентификации для установленного ранее сервера баз данных.
12. Нажмите на кнопку **Установить**, чтобы запустить установку.
13. После успешного завершения установки укажите, требуется ли запустить Консоль администрирования сразу после завершения работы мастера.

    Если вы выбрали открыть Kaspersky Security Center Web Console, откроется экран входа. Затем вы можете выполнить первоначальную настройку Сервера администрирования с помощью мастера первоначальной настройки.

    Вы можете запустить приложение Kaspersky Security Center Web Console, только если вы уже установили его. Вы не можете запустить приложение Kaspersky Security Center Web Console, если вы не установили его во время установки Kaspersky Security Center или отдельно.

14. В открывшемся окне Консоли администрирования выберите установленный Сервер администрирования.

15. Чтобы продолжить, в открывшемся окне с сертификатом Сервера администрирования нажмите на кнопку **Да**.

    Запустится мастер первоначальной настройки Сервера администрирования, если он не был запущен в веб-версии Консоли администрирования.

Устранение неисправностей

Если окно с сертификатом Сервера администрирования не отображается и появляются сообщения об ошибках подключения:

1. В Windows откройте окно **Службы** (**Панель управления** → **Администрирования** → **Службы**). Убедитесь, что запущены службы Агент администрирования Kaspersky Security Center и Сервер администрирования Kaspersky Security Center.

2. В Windows откройте окно **Просмотр событий** (**Панель управления** → **Администрирование** → **Просмотр событий**) и выберите **Журнал приложений и служб** → **Kaspersky Event Log**. Убедитесь, что в журнале событий отсутствуют записи об ошибках и присутствуют записи о событиях вида **Запущен Сервер администрирования <номер версии>**.

Установка Kaspersky Security Center Web Console

В этом разделе описано как установить Сервер Kaspersky Security Center Web Console (далее также Kaspersky Security Center Web Console) отдельно. Сначала необходимо установить СУБД и Сервер администрирования Kaspersky Security Center. Вы можете установить Kaspersky Security Center Web Console на том же устройстве, что и Kaspersky Security Center, или на другое.

Чтобы установить Kaspersky Security Center Web Console:

1. Запустите файл установки ksc-web-console-<номер_версии>.<номер сборки>.exe под учетной записью с правами администратора.

   Запускается мастер установки.

2. Выберите язык мастера установки.

3. В окне приветствия нажмите на кнопку **Далее**.

4. В окне **Лицензионное соглашение** прочитайте и примите условия Лицензионного соглашения. Установка продолжится после принятия Лицензионного соглашения, в противном случае кнопка **Далее** недоступна.

5. В окне **Папка назначения** выберите папку, в которую будет установлено приложение Kaspersky Security Center Web Console (по умолчанию %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console). Если такой папки нет, она будет создана автоматически в процессе установки.

   Вы можете изменить папку назначения с помощью кнопки **Обзор**.

6. В окне **Параметры подключения Kaspersky Security Center Web Console** укажите следующую информацию:

   - адрес Kaspersky Security Center Web Console (по умолчанию 127.0.0.1);
   - порт, который Kaspersky Security Center Web Console будет использовать для входящих подключений, то есть порт, который дает доступ к Kaspersky Security Center Web Console из браузера (по умолчанию 8080).

   Рекомендуется оставить значения адреса и порта по умолчанию.

   Нажмите на кнопку **Проверить**, если хотите проверить, доступен ли выбранный порт.

   Если вы хотите включить запись в журнал Kaspersky Security Center Web Console, выберите соответствующий параметр. Если этот параметр не выбран, файлы журнала Kaspersky Security Center Web Console не будут созданы.

7. В окне **Параметры учетной записи** укажите учетные записи и пароли.

   Рекомендуется использовать значения учетных записей по умолчанию.

8. В окне **Клиентский сертификат** выберите один из следующих параметров:

   - **Сформировать новый**. Этот вариант рекомендуется использовать, если у вас нет сертификата браузера.
   - **Выбрать существующий сертификат**. Вы можете выбрать этот вариант, если у вас уже есть сертификат браузера. В этом случае укажите путь к сертификату.
   - Если вы выбрали создать сертификат, при открытии Kaspersky Security Center Web Console, браузер может информировать вас о том, что подключение к Kaspersky Security Center Web Console не является приватным и что сертификат Kaspersky Security Center Web Console недействителен. Это предупреждение появляется потому, что сертификат Kaspersky Security Center Web Console является самоподписанным и автоматически генерируется Kaspersky Security Center. Чтобы удалить это предупреждение, создайте сертификат, доверенный в вашей инфраструктуре и соответствующий требованиям к пользовательским сертификатам. Далее выберите параметр **Выбрать существующий сертификат** в окне **Клиентский сертификат** и укажите путь к вашему пользовательскому сертификату.

   Сертификаты в формате PFX не поддерживаются приложением Kaspersky Security Center Web Console. Чтобы использовать такой сертификат, необходимо сначала преобразовать его в поддерживаемый формат PEM с помощью кроссплатформенной утилиты на основе OpenSSL, например, OpenSSL для Windows.

9. В окне **Доверенные Серверы администрирования** убедитесь, что ваш Сервер администрирования есть в списке, и нажмите на кнопку **Далее**, чтобы перейти к последнему окну мастера установки.

   Если нужно добавить в список новый Сервер администрирования, нажмите на кнопку **Добавить**. В открывшемся окне укажите свойства нового доверенного Сервера администрирования:

   - **Имя Сервера администрирования**

     Имя Сервера администрирования, которое будет отображаться в окне входа в Kaspersky Security Center Web Console.

   - **Адрес Сервера администрирования**

     IP-адрес устройства, на которое вы устанавливаете Сервер администрирования.

- **Порт Сервера администрирования**

  Порт OpenAPI, который Kaspersky Security Center Web Console, использует для подключения к Серверу администрирования (по умолчанию 13299).

- **Сертификат Сервера администрирования**

  Файл сертификата хранится на устройстве, на котором установлен Сервер администрирования. Путь к сертификату Сервера администрирования по умолчанию:

  - Для устройств с операционной системой Windows: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.
  - Для устройств с операционной системой Linux: /var/opt/kaspersky/klnagent_srv/1093/cert/.

  Если вы устанавливаете Kaspersky Security Center Web Console на то же устройство, где установлен Сервер администрирования, используйте один из указанных выше путей. Или скопируйте файл сертификата с устройства, на котором установлен Сервер администрирования, на устройство, на котором вы устанавливаете Kaspersky Security Center Web Console, и укажите локальный путь к сертификату.

10. В окне **Identity and Access Manager (IAM)** укажите, хотите ли вы установить Identity and Access Manager (далее также IAM). Если вы выбрали установку Identity and Access Manager, укажите следующие номера портов:

    - **KAS-порт администратора**. По умолчанию порт 4445 используется для получения конфигурации от Kaspersky Security Center Web Console для порта конечной точки авторизации OAuth2.0.
    - **Фасадный порт администратора**. По умолчанию порт 2444 используется для настройки Identity and Access Manager.
    - **Фасадный порт взаимодействия**. По умолчанию порт 2445 используется для подключения Kaspersky OSMP KAS Service к Kaspersky OSMP Facade Service.

    Вы можете изменить номера портов по умолчанию. В дальнейшем вы не сможете изменить их с помощью Kaspersky Security Center Web Console.

11. В последнем окне мастера установки нажмите на кнопку **Установить**, чтобы начать установку.

После успешного завершения установки на рабочем столе появляется ярлык и вы можете войти в Kaspersky Security Center Web Console.

Запускается мастер первоначальной настройки Сервера администрирования, если он не был запущен в Консоли администрирования, интегрированной в Microsoft Management Console.

Устранение неисправностей

Если Kaspersky Security Center Web Console не отображается в вашем браузере по указанному вами адресу, попробуйте сделать следующее:

1. Проверьте правильность указанного имени или IP-адреса устройства, на котором установлено приложение Kaspersky Security Center Web Console.
2. Убедитесь, что устройство, на котором вы работаете, имеет доступ к устройству, на котором установлено приложение Kaspersky Security Center Web Console.

3. Убедитесь, что параметры сетевого экрана устройства, на котором установлено приложение Kaspersky Security Center Web Console, разрешают входящие подключения через порт 8080 и для приложения node.exe.

4. В Windows откройте окно **Службы**. Убедитесь, что запущена Kaspersky Security Center Web Console.

5. Убедитесь, что у вас есть доступ к Kaspersky Security Center с помощью Консоли администрирования.

6. В Windows откройте окно **Просмотр событий** и выберите **Журнал приложений и служб → Kaspersky Event Log**. Убедитесь, что в журнале событий отсутствуют записи об ошибках.

Установка Kaspersky Security Center Web Console, подключенной к Серверу администрирования, установленного на узлах отказоустойчивого кластера "Лаборатории Касперского"

В этом разделе описывается установка Сервера Kaspersky Security Center Web Console (далее также Kaspersky Security Center Web Console), который подключается к Серверу администрирования, установленному на узлах отказоустойчивого кластера Kaspersky Security Center или узлах отказоустойчивого кластера Windows Server. Перед установкой Kaspersky Security Center Web Console установите СУБД и Сервер администрирования Kaspersky Security Center на узлы отказоустойчивого кластера Kaspersky Security Center или на узлы отказоустойчивого кластера Windows Server.

Если вы используете отказоустойчивый кластер Windows Server, не рекомендуется устанавливать Kaspersky Security Center Web Console на узел отказоустойчивого кластера. В случае сбоя узла вы потеряете доступ к Серверу администрирования.

Чтобы установить Kaspersky Security Center Web Console, которая подключается к Серверу администрирования, установленному на узлах отказоустойчивого кластера:

1. Выполните шаги из раздела Установка Kaspersky Security Center Web Console, начиная с шага 1 по шаг 8.

2. На шаге 9 в окне **Доверенные Серверы администрирования** нажмите на кнопку **Добавить**, чтобы добавить отказоустойчивый кластер в качестве доверенного Сервера администрирования.

   В открывшемся окне укажите следующие параметры:

   - **Имя Сервера администрирования**

     Имя кластера, которое будет отображаться в окне входа в Kaspersky Security Center Web Console.

   - **Адрес Сервера администрирования**

     В зависимости от типа отказоустойчивого кластера укажите адрес кластера:

     - **Отказоустойчивый кластер Kaspersky Security Center**. Укажите IP-адрес дополнительного сетевого адаптера в качестве адреса кластера, если вы создали адаптер при подготовке узлов кластера. В противном случае укажите IP-адрес стороннего балансировщика нагрузки, который вы используете.

     - **Отказоустойчивый кластер Windows Server**. Укажите адрес кластера, который вы получили при создании отказоустойчивого кластера Windows Server.

- **Порт Сервера администрирования**

  Порт OpenAPI, который Kaspersky Security Center Web Console, использует для подключения к Серверу администрирования (по умолчанию 13299).

- **Сертификат Сервера администрирования**

  Сертификат Сервера администрирования находится в общем хранилище данных отказоустойчивого кластера Kaspersky Security Center или отказоустойчивого кластера Windows Server. Путь по умолчанию к файлу сертификата: <shared data folder>\1093\cert\klserver.cer. Скопируйте файл сертификата из общего хранилища данных на устройство, на котором вы устанавливаете Kaspersky Security Center Web Console. Укажите локальный путь к сертификату Сервера администрирования.

3. Продолжите стандартную установку Kaspersky Security Center Web Console.

После завершения установки на рабочем столе появляется ярлык и вы можете войти в Kaspersky Security Center Web Console.

Обновление Kaspersky Security Center Web Console

Если вы хотите использовать новую версию Kaspersky Security Center Web Console, не удаляя установленный в данный момент экземпляр приложения, вы можете использовать стандартную процедуру обновления, предусмотренную в установщике Kaspersky Security Center Web Console.

Чтобы обновить Kaspersky Security Center Web Console:

1. Под учетной записью с правами администратора запустите ksc-web-console-<номер версии>.<номер сборки>.exe исполняемый файл, где <номер сборки> означает номер сборки Kaspersky Security Center Web Console, номер которой больше, чем у установленного вами экземпляра.

2. В открывшемся окне мастера установки выберите язык и нажмите на кнопку **OK**.

3. В окне приветствия выберите параметр **Обновить** и нажмите на кнопку **Далее**.

4. В окне **Лицензионное соглашение** прочитайте и примите условия Лицензионного соглашения. Установка продолжится после принятия Лицензионного соглашения, в противном случае кнопка **Далее** недоступна.

5. Выполните все шаги мастера установки, пока не завершите установку. В процессе установки вы также можете изменить параметры Kaspersky Security Center Web Console, которые вы указали при предыдущей установке. Нажмите на кнопку **Обновить** на шаге **Все готово для изменения Kaspersky Security Center Web Console**. Дождитесь, пока новые параметры вступят в силу, и на следующем шаге мастера установки нажмите на кнопку **Готово**. Вы также можете перейти по ссылке **Запустить Kaspersky Security Center Web Console в вашем браузере** для немедленного запуска обновленного экземпляра Kaspersky Security Center Web Console.

   > Изменение параметров Kaspersky Security Center Web Console при обновлении доступно только в Kaspersky Security Center Web Console версии 12.2 или выше.

   Приложение Kaspersky Security Center Web Console установлено.

Сертификаты для работы с Kaspersky Security Center Web Console

В разделе описано, как выпустить и заменить сертификаты для Kaspersky Security Center Web Console, а также как обновить сертификат Сервера администрирования, если Сервер взаимодействует с Kaspersky Security Center Web Console.

Перевыпуск сертификата для Kaspersky Security Center Web Console

Большинство браузеров ограничивает срок действия сертификата. Чтобы попасть в это ограничение, срок действия сертификата в Kaspersky Security Center Web Console равен 397 дням. Вы можете заменить существующий сертификат, полученный от доверенного центра сертификации (CA), при выпуске вручную нового самоподписанного сертификата. Вы также можете повторно выпустить устаревший сертификат Kaspersky Security Center Web Console.

> Автоматический перевыпуск сертификата для Kaspersky Security Center Web Console не поддерживается. Вам необходимо вручную перевыпустить сертификат.

Если вы уже используете самоподписанный сертификат, вы также можете перевыпустить его, обновив Kaspersky Security Center Web Console, используя стандартную процедуру в установщике (параметр **Обновить**).

Когда вы открываете Web Console, браузер может информировать вас о том, что подключение к Web Console не является приватным и что сертификат Web Console недействителен. Это предупреждение появляется потому, что сертификат Kaspersky Security Center Web Console является самоподписанным и автоматически генерируется Kaspersky Security Center. Чтобы удалить или предотвратить это предупреждение, можно выполнить одно из следующих действий:

- Укажите пользовательский сертификат при его повторном выпуске (рекомендуемый вариант). Создать сертификат, доверенный в вашей инфраструктуре и соответствующий требованиям к пользовательским сертификатам.
- Добавьте сертификат Web Console в список доверенных сертификатов браузера после перевыпуска сертификата. Рекомендуется использовать этот параметр только в том случае, если вы не можете создать пользовательский сертификат.

Чтобы выпустить новый сертификат при первой установке Kaspersky Security Center Web Console:

1. Запустите установку Kaspersky Security Center Web Console.
2. Выберите параметр **Сформировать новый** на шаге мастера установки **Клиентский сертификат** и нажмите на кнопку **Далее**.
3. Выполните все шаги мастера установки, пока не завершите установку.

   Новый сертификат для Kaspersky Security Center Web Console выписан со сроком действия 397 дней.

Чтобы перевыпустить просроченный сертификат Kaspersky Security Center Web Console:

1. Запустите исполняемый файл ksc-web-console-<номер_версии>.<номер сборки>.exe под учетной записью с правами администратора.

2. В открывшемся окне мастера установки выберите язык и нажмите на кнопку **OK**.

3. В окне приветствия выберите параметр **Перевыпустить сертификат** и нажмите на кнопку **Далее**.

4. На следующем шаге дождитесь завершения перенастройки Kaspersky Security Center Web Console и нажмите на кнопку **Готово**.

   Сертификат Kaspersky Security Center Web Console перевыпущен со сроком действия 397 дней.

Если вы используете Identity and Access Manager, вы также должны повторно выпустить все TLS-сертификаты для портов, которые используют Identity and Access Manager. В Kaspersky Security Center Web Console отображается уведомление об истечении срока действия сертификата. Следуйте инструкциям из уведомления.

Замена сертификата для Kaspersky Security Center Web Console

По умолчанию при установке Сервера Kaspersky Security Center Web Console сертификат браузера для приложения генерируется автоматически. Вы можете заменить автоматически сгенерированный сертификат на пользовательский.

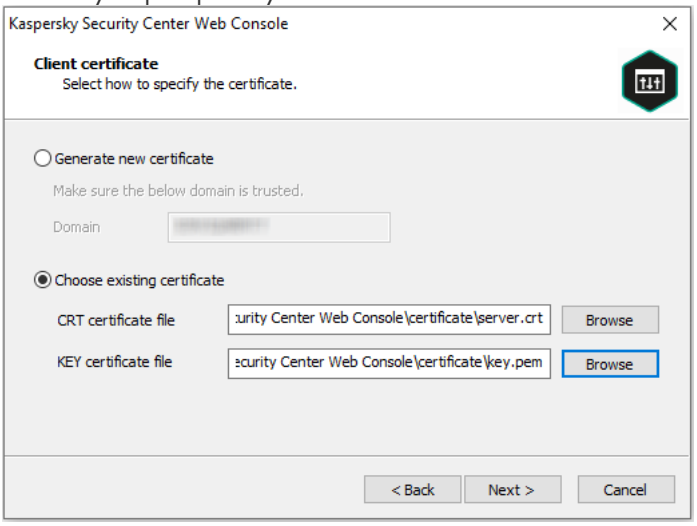
Чтобы заменить сертификат для Сервера Kaspersky Security Center Web Console на пользовательский сертификат:

1. Запустите на устройстве, на котором установлен Сервер Kaspersky Security Center Web Console, исполняемый файл ksc-web-console-<номер версии>.<номер сборки>.exe под учетной записью с правами администратора.

   Запускается мастер установки.

2. На первой странице мастера выберите параметр **Обновить**.

3. На странице **Клиентский сертификат** выберите параметр **Выбрать существующий сертификат** и укажите путь к пользовательскому сертификату.



Задание клиентского сертификата

4. На последней странице мастера нажмите на кнопку **Изменить**, чтобы применить новые параметры.

5. После успешного завершения настройки приложения нажмите на кнопку **Готово**.

Kaspersky Security Center Web Console работает с указанным сертификатом.

Указание сертификатов для доверенных Серверов администрирования в Kaspersky Security Center Web Console

Существующий сертификат Сервера администрирования автоматически заменяется новым до истечения срока действия сертификата. Вы также можете заменить существующий сертификат Сервера администрирования пользовательским. При каждом изменении сертификата новый сертификат должен быть указан в параметрах приложения Kaspersky Security Center Web Console. Иначе Kaspersky Security Center Web Console не сможет подключиться к Серверу администрирования.

Чтобы задать новый сертификат для Сервера администрирования:

1. На устройстве, на котором установлен Сервер администрирования, скопируйте файл сертификата, например, на запоминающее устройство.

   По умолчанию файл сертификата хранится в следующей папке:

   - Для устройств с операционной системой Windows: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.
   - Для устройств с операционной системой Linux: /var/opt/kaspersky/klnagent_srv/1093/cert/.

2. На устройстве, на котором установлено приложение Kaspersky Security Center Web Console, поместите файл сертификата в локальную папку.

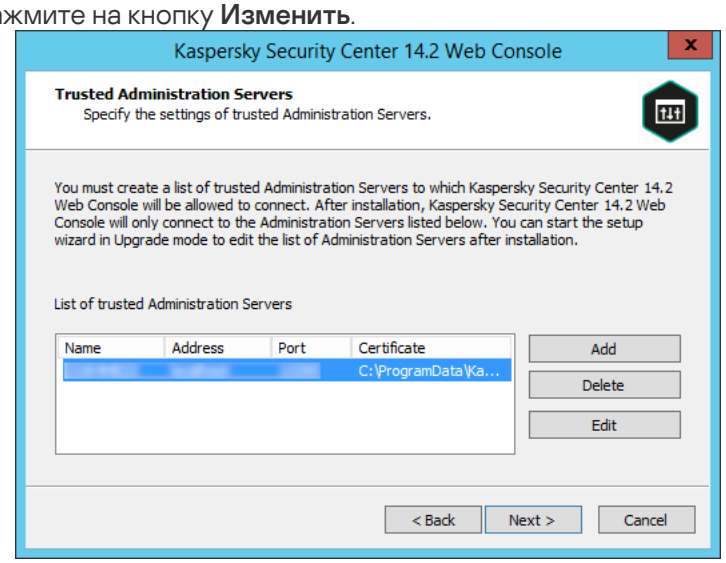
3. Запустите установочный файл ksc-web-console-<номер версии>.<номер сборки>.exe под учетной записью с правами администратора.

   Запускается мастер установки.

4. На странице мастера выберите параметр **Обновить**.

   Следуйте далее указаниям мастера.

5. На странице **Доверенные Серверы администрирования** выберите требуемый Сервер администрирования и нажмите на кнопку **Изменить**.



Задание доверенных Серверов администрирования

6. В открывшемся окне **Изменить Сервер администрирования** нажмите на кнопку **Обзор**, укажите путь к новому файлу сертификата и нажмите на кнопку **Обновить**, чтобы применить изменения.

7. На странице **Все готово для изменения Kaspersky Security Center Web Console** мастера нажмите на кнопку **Обновить**, чтобы начать обновление.

8. После успешного завершения настройки приложения нажмите на кнопку **Готово**.

9. Войдите в Kaspersky Security Center Web Console.

Kaspersky Security Center Web Console работает с указанным сертификатом.

Преобразование сертификата из формата PFX в формат PEM

Чтобы использовать сертификат формата PFX в Kaspersky Security Center Web Console, вам необходимо предварительно преобразовать его в формат PEM с помощью любой кроссплатформенной утилиты на основе OpenSSL.

Чтобы преобразовать сертификат из формата PFX в формат PEM в операционной системе Windows:

1. В кроссплатформенной утилите на основе OpenSSL выполните следующие команды:

   ```
   openssl pkcs12 -in <имя_файла.pfx> -clcerts -nokeys -out server.crt
   openssl pkcs12 -in <имя_файла.pfx> -nocerts -nodes -out key.pem
   ```

   В результате вы получаете открытый ключ в виде файла .crt и закрытый ключ в виде защищенного парольной фразой файла .pem.

2. Убедитесь, что файлы .crt и .pem сгенерированы в той же папке, где хранится .pfx файл.

3. Если файл .crt или .pem содержит "пакет атрибутов", удалите эти атрибуты с помощью любого удобного текстового редактора и сохраните файл.

4. Перезапустите службу Windows.

5. Kaspersky Security Center Web Console не поддерживает сертификаты, защищенные парольной фразой. Поэтому выполните команду в кроссплатформенной утилите на основе OpenSSL, чтобы удалить парольную фразу из файла .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Не используйте одно и то же имя для входных и выходных файлов .pem.

   В результате новый файл .pem не зашифрован. Вводить парольную фразу для его использования не нужно.

Файлы .crt и .pem готовы к использованию, поэтому вы можете указать их в мастере установки Kaspersky Security Center Web Console.

Чтобы преобразовать сертификат из формата PFX в формат PEM в операционной системе Linux:

1. В кроссплатформенной утилите на основе OpenSSL выполните следующие команды:

   ```
   openssl pkcs12 -in <имя_файла.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <имя_файла.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Убедитесь, что файл сертификата и закрытый ключ сгенерированы в той же директории, где хранится файл PFX.

3. Kaspersky Security Center Web Console не поддерживает сертификаты, защищенные парольной фразой. Поэтому выполните команду в кроссплатформенной утилите на основе OpenSSL, чтобы удалить парольную фразу из файла .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Не используйте одно и то же имя для входных и выходных файлов .pem.

   В результате новый файл .pem не зашифрован. Вводить парольную фразу для его использования не нужно.

Файлы .crt и .pem готовы к использованию, поэтому вы можете указать их в мастере установки Kaspersky Security Center Web Console.

Перенос данных из Kaspersky Security Center Windows

В этом разделе описан перенос данных управляемых устройств и связанных с ними объектов (политик, задач, групп, тегов и других объектов) из Kaspersky Security Center Windows.

- Kaspersky Security Center Cloud Console
- Kaspersky Security Center Linux

Перенос данных в Kaspersky Security Center Cloud Console

Вы можете выполнить перенос данных из приложения Kaspersky Security Center Web Console в Kaspersky Security Center Cloud Console вручную. После этого вы получаете доступ к Серверу администрирования и системе управления базами данных (СУБД), которые размещены в инфраструктуре "Лаборатории Касперского". Вам не нужен физический сервер или СУБД: и то, и другое обслуживается за вас экспертами "Лаборатории Касперского".

Вы можете перенести данные управляемых устройств с операционными системами Windows, Linux или macOS под управление Kaspersky Security Center Cloud Console. Если в вашей сети есть иерархия Серверов администрирования, вы можете сохранить ее в Kaspersky Security Center Cloud Console. Кроме того, вы можете перенести:

- Задачи и политики управляемых приложений.
- Глобальные задачи.
- Пользовательские выборки устройств.
- Структуру групп администрирования и входящие в нее устройства.
- Теги, назначенные устройствам, данные которых вы переносите.

После завершения переноса данных вы сможете управлять устройствами с помощью Kaspersky Security Center Cloud Console. При этом переносимые объекты сохраняются, а Агент администрирования переустанавливается на все управляемые устройства.

Информацию о том, как выполнить перенос данных, и список предварительных требований см. в *справке Kaspersky Security Center Cloud Console*.

Перенос данных в Kaspersky Symphony XDR

Следуя этому сценарию, вы можете передать структуру группы администрирования, включая управляемые устройства и другие объекты группы (политики, задачи, глобальные задачи, теги и выборки устройств) из Kaspersky Security Center Windows под управление Kaspersky Symphony XDR.

Ограничения:

- Перенос данных возможен только с Kaspersky Security Center 14.2 Windows в Kaspersky Symphony XDR, начиная с версии 1.0.
- Вы можете выполнить этот сценарий только с помощью Kaspersky Security Center Web Console.

Этапы

Сценарий переноса данных состоит из следующих этапов:

1. **Выберите способ переноса данных**

Вы переносите данные в Kaspersky Symphony XDR с помощью мастера переноса данных. Шаги мастера переноса данных зависят от того, организованы ли Серверы администрирования Kaspersky Security Center Windows и Kaspersky Symphony XDR в иерархию:

- Перенос данных с использованием иерархии Серверов администрирования

  Выберите этот вариант, если Сервер администрирования Kaspersky Security Center Windows является подчиненным по отношению к Серверу администрирования Kaspersky Symphony XDR. Вы управляете процессом переноса данных и переключаетесь между Серверами в рамках одного экземпляра Консоли Kaspersky Security Center. Если вы предпочитаете этот вариант, вы можете организовать Серверы администрирования в иерархию, чтобы упростить процедуру переноса данных. Для этого перед началом переноса данных создайте иерархию.

- Перенос данных с помощью файла экспорта (ZIP-архив)

  Выберите этот вариант, если Серверы администрирования Kaspersky Security Center Windows и Kaspersky Symphony XDR не организованы в иерархию. Вы управляете процессом переноса данных с помощью двух экземпляров Консоли, одного экземпляра Kaspersky Security Center Windows и другого Консоли Kaspersky Security Center. В этом случае вы используете файл экспорта, который вы создали и загрузили при экспорте из Kaspersky Security Center Windows, и импортируете этот файл в Kaspersky Symphony XDR.

2. **Экспорт данных из Kaspersky Security Center Windows**

   Откройте Kaspersky Security Center Windows и запустите мастер переноса данных.

3. **Импорт данных в Kaspersky Symphony XDR**

   Продолжите работу мастера передачи данных, чтобы импортировать экспортированные данные в Kaspersky Symphony XDR.

   Если Серверы организованы в иерархию, импорт начинается автоматически после успешного экспорта в том же мастере. Если Серверы не выстроены в иерархию, вы продолжите работу мастера передачи данных после перехода на Kaspersky Symphony XDR.

4. **Выполнение дополнительных действий для переноса объектов и параметров из Kaspersky Security Center Windows в Kaspersky Symphony XDR вручную (необязательный шаг)**

   Вы также можете перенести объекты и параметры, которые невозможно передать с помощью мастера переноса данных. Например, вы можете дополнительно сделать следующее:

   - Настроить глобальные задачи Сервера администрирования.
   - Настроить параметры политики Агента администрирования.
   - Создать инсталляционные пакеты приложений.
   - Создать виртуальные Серверы администрирования.
   - Назначить и настроить точки распространения.
   - Создать правила перемещения устройств.
   - Настроить правила автоматического назначения тегов устройствам.
   - Создать категории приложений.

5. **Переместить импортированные управляемые устройства под управление Kaspersky Symphony XDR**

Для завершения переноса данных переместите импортированные управляемые устройства под управление Kaspersky Symphony XDR. Вы можете воспользоваться одним из следующих способов:

- С помощью групповой задачи Kaspersky Security Center

  Используйте задачу Сменить Сервер администрирования, чтобы сменить Сервер администрирования на другой для конкретных клиентских устройств.

- С помощью утилиты klmover.

  Используйте утилиту klmover и укажите параметры подключения для нового Сервера администрирования.

- С помощью установки или переустановки Агента администрирования на управляемые устройства.

  Создайте инсталляционный пакет Агента администрирования и укажите параметры подключения для нового Сервера администрирования в свойствах инсталляционного пакета. Используя инсталляционный пакет, установите Агент администрирования на импортированные управляемые устройства с помощью задачи удаленной установки.

  Вы также можете создать и использовать автономный инсталляционный пакет для локальной установки Агента администрирования.

6. **Убедитесь, что управляемые устройства отображаются на новом Сервере администрирования.**

   На Сервере администрирования Kaspersky Symphony XDR откройте список управляемых устройств (**Активы (Устройства)** → **Управляемые устройства**) и проверьте значения в столбцах **Видимо в сети**, **Агент администрирования установлен** и **Последнее подключение к Серверу администрирования**.

Другие способы переноса данных

Помимо мастера переноса данных, вы также можете переносить определенные задачи и политики:

- Экспортируйте задачи из Kaspersky Security Center Windows, а затем импортируйте задачи в Kaspersky Symphony XDR.
- Экспортируйте политики из Kaspersky Security Center Windows, а затем импортируйте политики в Kaspersky Symphony XDR. Связанные профили политик экспортируются и импортируются вместе с выбранными политиками.

Перенос данных в приложение Kaspersky Security Center Linux

Перенос данных из Kaspersky Security Center Windows в Kaspersky Security Center Linux можно выполнить с помощью резервного копирования данных Сервера администрирования (с использованием утилиты klbackup) и мастера переноса данных.

Таблица ниже позволяет сравнить основные возможности и ограничения переноса данных с использованием резервного копирования данных Сервера администрирования и мастера переноса данных, чтобы решить, какой способ больше подходит для вашей организации.

Сравнение способов переноса данных

Параметры	Резервное копирование данных Сервера администрирования	Мастер переноса данных
Процесс переноса данных	Создание полной резервной копии данных Сервера администрирования Kaspersky Security Center Windows и ее восстановление на Сервере администрирования Kaspersky Security Center Linux.	Выбор и экспорт данных Сервера администрирования для переноса, импорт этих данных на Сервер администрирования Kaspersky Security Center Linux и переключение управляемых устройств под управление Kaspersky Security Center Linux.
Особенности переноса данных	• Перенос всех данных Сервера администрирования. • Перенос любого количества управляемых устройств. • Используется для получения полной копии данных Сервера администрирования Kaspersky Security Center Windows и переноса их на Сервер администрирования Kaspersky Security Center Linux.	• Частичное резервное копирование данных Сервера администрирования. • Возможен выбор объектов для переноса. • Группа администрирования или ее подгруппа, которую нужно перенести, может содержать не более 10 000 устройств. • Используется для частичного переноса данных Сервера администрирования, включая только групповые объекты в пределах области переноса данных; групповые объекты вне области переноса данных необходимо восстановить вручную.
Область действия переноса данных	Полный перенос данных Сервера администрирования с неограниченным количеством управляемых устройств.	• Структура групп администрирования. • Управляемые устройства, включенные в группы администрирования (**не более 10 000 устройств**). • Теги, присвоенные перенесенным устройствам. • Глобальные задачи Агента администрирования и управляемые приложения (не для Сервера администрирования). • Групповые задачи Агента администрирования и управляемых приложений. • Политики управляемых приложений. • Шаблоны отчетов. • Роли пользователей. • Внутренние пользователи и группы безопасности. • Пользовательские категории приложений пополняемые вручную. • Пользовательские выборки устройств.
Область действия, не подлежащая переносу	—	• Глобальные задачи Сервера администрирования. • События, сохраненные на Сервере администрирования. • Хранилище дистрибутивов приложений для удаленной установки. • Сертификат Сервера администрирования. • Лицензионные ключи, используемые Сервером администрирования и управляемыми приложениями. • Виртуальные Серверы администрирования. • Параметры политики Агента администрирования. • Правила перемещения устройств. • Правила автоматического назначения тегов устройствам. • Точки распространения. • Параметры приложения "Лаборатории Касперского" сохраненные на Сервере администрирования.
Версии Kaspersky Security Center, поддерживающие перенос данных	• Любая поддерживаемая версия Kaspersky Security Center Windows. • Kaspersky Security Center Linux версии 15.2 или выше.	• Kaspersky Security Center Windows версии 14.2 или выше. • Kaspersky Security Center Linux версии 15 или выше.
СУБД, между которыми можно выполнять перенос данных	• Microsoft SQL Server → MySQL, MariaDB. • Microsoft SQL Server → PostgreSQL, Postgres Pro (только для переноса данных из Kaspersky Security Center Windows версии 14.2 или выше с установленным патчем в Kaspersky Security Center Linux версии 15.3 или выше). • MySQL → MySQL, MariaDB. • MariaDB → MySQL, MariaDB. • PostgreSQL → PostgreSQL. Postgres Pro → Postgres Pro (только для переноса данных из Kaspersky Security Center Windows версии 15.1 или выше в Kaspersky Security Center Linux версии 16 или выше).	Перенос данных между поддерживаемыми СУБД без ограничений.

Перенос данных в Kaspersky Security Center Linux с использованием резервной копии данных Сервера администрирования

Вы можете использовать резервную копию данных для переноса данных Сервера администрирования Kaspersky Security Center Windows в Kaspersky Security Center Linux. Перед переносом данных убедитесь, что необходимые функции Kaspersky Security Center Windows поддерживаются в Kaspersky Security Center Linux.

Ограничения:

- Перенос данных возможен между следующими СУБД:
  - Microsoft SQL Server → MySQL, MariaDB.
  - Microsoft SQL Server → PostgreSQL, Postgres Pro.
  - MySQL → MySQL, MariaDB.
  - MariaDB → MySQL, MariaDB.
  - PostgreSQL → PostgreSQL.
  - Postgres Pro → Postgres Pro.
- Перенос данных Сервера администрирования, хранящихся в базе данных Microsoft SQL Server, MySQL или MariaDB, в MySQL или MariaDB поддерживается для переноса из любой поддерживаемой версии Kaspersky Security Center Windows в Kaspersky Security Center Linux версии 15.2 и выше.
- При переносе данных из Kaspersky Security Center Windows версии 15.1 и выше в Kaspersky Security Center Linux версии 16 и выше поддерживается перенос данных Сервера администрирования, хранящихся в базе данных PostgreSQL в PostgreSQL или Postgres Pro в Postgres Pro.
- При переносе данных из Kaspersky Security Center Windows версии 14.2 и выше в Kaspersky Security Center Linux версии 15.3 и выше поддерживается перенос данных Сервера администрирования, хранящихся в базе данных Microsoft SQL Server, в PostgreSQL или Postgres Pro.

  Для поддержки переноса данных в PostgreSQL или Postgres Pro вы можете обновить Kaspersky Security Center Windows до версии 15.1.0.28509.
- Если вы используете MySQL или MariaDB в качестве СУБД для Kaspersky Security Center Windows и для Kaspersky Security Center Linux, параметр `lower_case_table_names` должен совпадать в текущей и новой СУБД.

  Прежде чем приступить к созданию резервной копии данных, проверьте параметр `lower_case_table_names`. Затем при установке MySQL или MariaDB для Kaspersky Security Center Linux, вам нужно установить то же значение параметра, которое указано для этого параметра для Windows.

Этапы

Перенос данных с использованием резервного копирования данных Сервера администрирования состоит из следующих этапов:

1. **Проверка наличия у вас внутренней учетной записи администратора, под которой вы можете выполнить вход на Сервер администрирования**

   Для входа на Сервер администрирования Kaspersky Security Center Linux будет использоваться учетная запись администратора. Если у вас нет такой учетной записи и вы вошли только под локальной учетной записью Windows или под доменной учетной записью, то после восстановления резервной копии вы не сможете выполнить вход на Сервер администрирования Kaspersky Security Center Linux. Сервер администрирования Kaspersky Security Center Linux не поддерживает вход с использованием локальной учетной записи Windows. Вход под доменной учетной записью возможен, но может потребовать дополнительной настройки Сервера администрирования.

   Если у вас нет учетной записи администратора, вам нужно будет ее создать после того, как вы восстановите резервную копию с помощью утилиты kladduser.

2. **Создание актуальной резервной копии данных Сервера администрирования Kaspersky Security Center Windows**

   В зависимости от типа СУБД, используемой Kaspersky Security Center Windows и Kaspersky Security Center Linux, выполните одно из следующих действий:

   - Для переноса данных с MySQL или MariaDB на MySQL или MariaDB: создайте резервную копию с помощью утилиты klbackup или задачи резервного копирования данных на устройстве, на котором установлен Сервер администрирования.
   - Для переноса данных из PostgreSQL в PostgreSQL и Postgres Pro в Postgres Pro: создайте резервную копию данных с помощью утилиты klbackup или задачи резервного копирования данных на устройстве, на котором установлен Сервер администрирования.
   - Для переноса данных Microsoft SQL Server в MySQL или MariaDB: создайте резервную копию данных с помощью утилиты klbackup с включенным параметром **Перенос данных в формате MySQL/MariaDB**.
   - Для переноса данных Microsoft SQL Server в PostgreSQL или Postgres Pro:

     1. Обновите Kaspersky Security Center Windows до версии 15.1.0.28509.
     2. Создайте резервную копию данных с помощью утилиты klbackup.

        Если вы запускаете утилиту klbackup из командной строки, используйте флаг `-migrate postgres`.

        Если вы используете интерфейс утилиты klbackup, включите параметр **Перенести в формат Postgres**.

   После создания резервной копии данных отключите Сервер администрирования Kaspersky Security Center Windows от сети.

3. **Подготовка нового устройства к установке Kaspersky Security Center Linux**

На этом этапе сценария выполните следующее:

1. Выберите новое устройство, на которое будет установлен Сервер администрирования. Это устройство должно соответствовать аппаратным и программным требованиям. Проверьте, что порты, используемые на Сервере администрирования доступны.

2. Назначьте новому устройству тот же адрес.

   Новому Серверу администрирования можно присвоить имя NetBIOS, FQDN и статический IP-адрес. Это зависит от того, какой адрес Сервера администрирования был установлен в инсталляционном пакете Агента администрирования, когда были развернуты Агенты администрирования. Также вы можете использовать адрес подключения, определяющий Сервер администрирования, к которому подключается Агент администрирования (вы можете получить этот адрес на управляемых устройствах с помощью утилиты klnagchk).

4 Установка и настройка СУБД

На этом этапе сценария выполните следующее:

1. Выберите тип СУБД, который обеспечивает оптимальную производительность. Учитывайте количество сетевых устройств, топологию сети и нагрузку на сеть. Вы можете выбрать одну из поддерживаемых СУБД.

2. Установите СУБД в соответствии с типом СУБД, выбранным при создании резервной копии. Подробнее о том как установить выбранную СУБД, см. в документации к этой СУБД.

   > Новая версия базы данных не должна быть ниже текущей.

3. Настройте СУБД для работы с Kaspersky Security Center Linux.

5 Установка Kaspersky Security Center Linux

Установите Kaspersky Security Center Linux на новом устройстве.

Внутренняя учетная запись администратора, созданная во время установки, а также другие объекты (группы, политики, задачи, пользователи), созданные до восстановления данных Сервера администрирования из резервной копии, после восстановления будут утеряны. Эти объекты будут заменены объектами из резервной копии.

6 Восстановление данных Сервера администрирования из резервной копии

На этом этапе сценария выполните следующее:

1. Восстановите данные Сервера администрирования на новом устройстве с помощью утилиты klbackup.

2. Если у вас не было внутренней учетной записи администратора, под которой вы выполнили вход на Сервер администрирования Kaspersky Security Center Windows, и вы использовали локальную учетную запись Windows или доменную учетную запись, создайте учетную запись администратора с помощью утилиты kladduser следующим образом:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>
   ```

где <password> соответствует следующим требованиям:

- Пароль пользователя не может содержать менее 8 или более 256 символов.
- Пароль должен содержать символы как минимум трех групп из списка ниже:
  - верхний регистр (A–Z);
  - нижний регистр (a–z);
  - числа (0–9);
  - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).

7. **Установка Сервера Kaspersky Security Center Web Console или Сервера администрирования**

   На этом этапе сценария выполните следующее:

   1. Установите Kaspersky Security Center Web Console.

      Если приложение Kaspersky Security Center Web Console было установлено ранее, переустановите его с тем же файлом ответов.

      Выполните вход в Kaspersky Security Center Web Console под внутренней учетной записью администратора.

      Процесс инициализации данных обычно занимает до 15 минут после восстановления данных Сервера администрирования, но время зависит от производительности оборудования и размера данных Сервера администрирования. В течение этого периода Kaspersky Security Center Web Console может не подключаться и отображать ошибки.

   2. Проверьте функциональность основных функций Сервера администрирования после завершения инициализации данных в базе данных. Убедитесь, что Сервер администрирования синхронизируется с управляемыми устройствами и данные Сервера администрирования восстановлены.

   3. Выполните опрос контроллеров доменов для восстановления информации о структуре домена, учетных записях пользователей, группах безопасности и о DNS-именах устройств, входящих в домены.

   4. При необходимости удалите Сервер администрирования и сервер баз данных с предыдущего устройства.

      Не должно быть нескольких Серверов администрирования в одной сети с одним и тем же адресом подключения и сертификатом Сервера администрирования.

Администратор имеет доступ к данным Сервера администрирования и управляемым устройствам, которые были в Kaspersky Security Center Windows с учетом функциональности, поддерживаемой в Kaspersky Security Center Linux.

Перенос данных в Kaspersky Security Center Linux с помощью мастера переноса данных

Следуя этому сценарию, вы можете переместить структуру групп администрирования, включая управляемые устройства и другие объекты группы (политики, задачи, глобальные задачи, теги и выборки устройств) из Kaspersky Security Center Windows под управление Kaspersky Security Center Linux. Перед переносом данных убедитесь, что необходимые функции Kaspersky Security Center Windows поддерживаются в Kaspersky Security Center Linux.

Ограничения:

- Перенос данных возможен только из Kaspersky Security Center Windows версии 14.2 и выше в Kaspersky Security Center Linux версии 15 и выше.
- Вы можете выполнить этот сценарий только с помощью Kaspersky Security Center Web Console.

Этапы

Сценарий переноса данных состоит из следующих этапов:

1. **Выберите способ переноса данных**

   Вы переносите данные в Kaspersky Security Center Linux с помощью мастера переноса данных. Действия мастера переноса данных зависят от того, организованы ли Серверы администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux в иерархию:

   - Перенос данных с использованием иерархии Серверов администрирования

     Выберите этот параметр, если Сервер администрирования Kaspersky Security Center Windows является подчиненным по отношению к Серверу администрирования Kaspersky Security Center Linux. Вы управляете процессом переноса данных и переключаетесь между Серверами в рамках одного экземпляра Kaspersky Security Center Web Console. Если вы предпочитаете этот вариант, вы можете организовать Серверы администрирования в иерархию, чтобы упростить процедуру переноса данных. Для этого создайте иерархию перед началом переноса данных.

   - Перенос данных с помощью файла экспорта (ZIP-архив)

     Выберите этот параметр, если Серверы администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux не организованы в иерархию. Вы управляете процессом переноса данных с помощью двух экземпляров Kaspersky Security Center Web Console, одного экземпляра Kaspersky Security Center Windows и другого Kaspersky Security Center Linux. В этом случае вы будете использовать файл экспорта, который вы создали и загрузили во время экспорта из Kaspersky Security Center Windows, и импортировать этот файл в Kaspersky Security Center Linux.

2. **Создание резервной копии сертификата и закрытого ключа Сервера администрирования Kaspersky Security Center Windows (необязательный шаг)**

   Возможно, вы захотите поместить управляемые устройства под управление Сервера администрирования Kaspersky Security Center Linux, восстановив сертификат и закрытый ключ Сервера администрирования из резервной копии. В этом случае создайте резервную копию сертификата и закрытого ключа Сервера администрирования Kaspersky Security Center Windows. Затем на шаге 6 восстановите сертификат и закрытый ключ.

3. **Экспорт данных из Kaspersky Security Center Windows**

   Откройте Kaspersky Security Center Windows и запустите мастер переноса данных.

4. **Импорт данных в приложение Kaspersky Security Center Linux**

   Продолжите работу мастера переноса данных, чтобы импортировать экспортированные данные в Kaspersky Security Center Linux. Если Серверы организованы в иерархию, импорт начинается автоматически после успешного экспорта в том же мастере. Если Серверы не выстроены в иерархию, вы продолжите работу мастера переноса данных после перехода на Kaspersky Security Center Linux.

5. **Выполнение дополнительных действий для переноса объектов и параметров из Kaspersky Security Center Windows в Kaspersky Security Center Linux вручную (необязательный шаг)**

Также можно перенести объекты и параметры, которые вы не можете передать с помощью мастера переноса данных. Например, вы можете дополнительно сделать следующее:

- Перенести лицензионные ключи, используемые Сервером администрирования и управляемыми приложениями.
- Настроить глобальные задачи Сервера администрирования.
- Настроить параметры политики Агента администрирования.
- Создать инсталляционные пакеты приложений.
- Создать виртуальные Серверы администрирования.
- Назначить и настроить точки распространения.
- Создать правила перемещения устройств.
- Настроить правила автоматического назначения тегов устройствам.
- Создать категории приложений.

6. **Переместить импортированные управляемые устройства под управление Kaspersky Security Center Linux**

   Завершите перенос данных, переместите импортированные управляемые устройства под управление Kaspersky Security Center Linux. Вы можете воспользоваться одним из следующих способов:

   - С помощью утилиты klmover.

     Используйте утилиту klmover и укажите параметры подключения для нового Сервера администрирования.

   - С помощью задачи *Смена сервера администрирования*.

     Создайте задачу *Сменить Сервер администрирования*, укажите импортированные управляемые устройства, новый Сервер администрирования и другие параметры задачи. Затем запустите задачу, чтобы поместить управляемые устройства под управление Сервера администрирования Kaspersky Security Center Linux.

   - С помощью удаления (если уже установлен) и дальнейшей установки Агента администрирования на управляемых устройствах.

     Создайте инсталляционный пакет Агента администрирования и укажите параметры подключения для нового Сервера администрирования в свойствах инсталляционного пакета. Удалите Агент администрирования на импортированных управляемых устройствах, а затем используйте инсталляционный пакет для установки Агента администрирования на этих устройствах с помощью задачи удаленной установки. Вы также можете создать и использовать автономный инсталляционный пакет для локальной установки Агента администрирования. Подробнее см. в разделе Переключение управляемых устройств под управление Kaspersky Security Center Linux.

- С помощью восстановления сертификата и закрытого ключа Сервера администрирования из резервной копии (только для переноса данных в Kaspersky Security Center Linux 15.1 и выше).

  Назначьте устройству с Сервером администрирования Kaspersky Security Center Linux тот же сетевой адрес, что и у устройства с Сервером администрирования Kaspersky Security Center Windows. Запустите утилиту klbackup с параметром `-cert_only`, чтобы восстановить сертификат Сервера администрирования и закрытый ключ из резервной копии, сохраненной на шаге 2. Выполните следующую команду в командной строке: `/opt/kaspersky/ksc64/sbin/klbackup -path <путь к резервной копии сертификата Сервера администрирования> -restore -cert_only`. Подробнее см. Использование утилиты klbackup для переключения управляемых устройств под управление другого Сервера администрирования.

7. **Обновите Агент администрирования до последней версии.**

   Рекомендуется обновить Агент администрирования для Linux до той же версии, что и Kaspersky Security Center.

8. **Убедитесь, что управляемые устройства отображаются на новом Сервере администрирования.**

   На Сервере администрирования Kaspersky Security Center Linux откройте список управляемых устройств (**Активы (Устройства)** → **Управляемые устройства**) и проверьте значения в столбцах **Видимо в сети**, **Агент администрирования установлен** и **Последнее подключение к Серверу администрирования**.

Другие способы переноса данных

Помимо мастера переноса данных, вы также можете переносить определенные задачи и политики:

- Экспортируйте задачи из Kaspersky Security Center Windows, а затем импортируйте задачи в Kaspersky Security Center Linux.
- Экспортируйте определенные политики из Kaspersky Security Center Windows, а затем импортируйте политики в Kaspersky Security Center Linux. Связанные профили политик экспортируются и импортируются вместе с выбранными политиками.

Экспорт групповых объектов из Kaspersky Security Center Windows

Для переноса структуры группы администрирования, которая включает управляемые устройства и другие объекты группы из Kaspersky Security Center Windows в Kaspersky Security Center Linux, вам сначала необходимо выбрать данные для экспорта и создать файл экспорта. Файл экспорта содержит информацию обо всех групповых объектах, которые вы хотите перенести. Файл экспорта будет использоваться для последующего импорта в Kaspersky Security Center Linux.

Вы можете экспортировать следующие объекты:

- Задачи и политики управляемых приложений.
- Глобальные задачи.
- Пользовательские выборки устройств.
- Структуру групп администрирования и входящие в нее устройства.
- Теги, назначенные устройствам, данные которых вы переносите.

Перед началом экспорта прочтите общую информация о переносе данных в Kaspersky Security Center Linux. Выберите способ переноса данных: с использованием или без использования иерархии Серверов администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux.

Чтобы экспортировать управляемые устройства и связанные групповые объекты с помощью мастера переноса данных:

1. В зависимости от того, организованы ли в иерархию Серверы администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux, выполните одно из следующих действий:

   - Если Серверы выстроены в иерархию, откройте Kaspersky Security Center Web Console и переключитесь на Сервер администрирования Kaspersky Security Center Windows.

   - Если Серверы не организованы в иерархию, откройте Kaspersky Security Center Web Console, подключенную к Kaspersky Security Center Windows.

2. В главном окне приложения перейдите в раздел **Операции** → **Перенос данных**.

3. Чтобы запустить мастер и следовать его шагам, выберите, куда вы хотите перенести свои данные и параметры.

   - Если вы хотите перенести свои данные и параметры в Kaspersky Security Center Cloud Console, выберите параметр **Перенос данных в Kaspersky Security Center Cloud Console**.

   - Если вы хотите перенести свои данные и параметры в Kaspersky Security Center Linux или Kaspersky Symphony XDR, выберите параметр **Перенос данных в Kaspersky Security Center Linux или Open Single Management Platform**.

4. Выберите группу или подгруппу администрирования, которую вы хотите экспортировать. Обратите внимание, что в выбранной группе или подгруппе администрирования должно быть не более 10 000 устройств.

5. Выберите управляемые приложения, задачи и политики которых будут экспортированы. Выберите только те приложения, которые поддерживаются Kaspersky Security Center Linux. Объекты неподдерживаемых приложений все равно будут экспортированы, но не будут работать.

6. Используйте ссылки слева, чтобы выбрать глобальные задачи, выбранные устройства и отчеты для экспорта. Ссылка **Группировать объекты** позволяет исключить из экспорта роли пользователей, внутренних пользователей и группы безопасности, а также пользовательские категории приложений.

Файл экспорта (ZIP-архив) создан. В зависимости от того, выполняете ли вы перенос данных с поддержкой иерархии Сервера администрирования, файл экспорта сохраняется следующим образом:

- Если Серверы выстроены в иерархию, файл экспорта сохраняется во временную папку на Сервере Kaspersky Security Center Web Console.

- Если Серверы не организованы в иерархию, файл экспорта загружается на ваше устройство.

При переносе данных с поддержкой иерархии Сервера администрирования импорт начинается автоматически после успешного экспорта. При переносе данных без поддержки иерархии Сервера администрирования вы можете вручную импортировать сохраненный файл экспорта в Kaspersky Security Center Linux.

Импорт файла экспорта в Kaspersky Security Center Linux

Чтобы передать информацию об управляемых устройствах, объектах и их параметрах, которые вы экспортировали из Kaspersky Security Center Windows, вам нужно импортировать ее в приложение Kaspersky Security Center Linux или Kaspersky Symphony XDR.

Чтобы импортировать управляемые устройства и связанные групповые объекты с помощью мастера переноса данных:

1. В зависимости от того, организованы ли в иерархию Серверы администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux, выполните одно из следующих действий:

   - Если Серверы организованы в иерархию, переходите к следующему шагу мастера переноса данных после завершения экспорта. Импорт начнется автоматически после успешного экспорта в этом мастере (см. шаг 2 этой инструкции).

   - Если Серверы не организованы в иерархию:

     a. Откройте приложение Kaspersky Security Center Web Console, подключенное к Kaspersky Security Center Linux или к Kaspersky Symphony XDR.

     b. В главном окне приложения перейдите в раздел **Операции** → **Перенос данных**.

     c. Выберите файл экспорта (ZIP-архив), который вы создали и загрузили при экспорте из Kaspersky Security Center Windows. Начнется загрузка файла экспорта.

2. После успешной загрузки файла экспорта вы можете продолжить импорт. Если вы хотите указать другой файл для экспорта, перейдите по ссылке **Изменить** и выберите нужный файл.

3. Отобразится вся иерархия групп администрирования Kaspersky Security Center Linux.

   Установите флажок рядом с целевой группой администрирования, в которой необходимо восстановить объекты экспортированной группы администрирования (управляемые устройства, политики, задачи и другие объекты группы).

4. Начнется импорт объектов группы. Свернуть мастер переноса данных и выполнять любые параллельные операции во время импорта невозможно. Дождитесь, пока значки (🔄) рядом со всеми пунктами в списке объектов заменятся на зеленые флажки (✓) и импорт завершится.

5. Когда импорт завершится, экспортированная структура групп администрирования, включая сведения об устройствах, появится в целевой группе администрирования, которую вы выбрали. Если имя восстанавливаемого объекта совпадает с именем существующего объекта, к восстановленному будет добавлен дополнительный суффикс.

Если в перенесенной задаче указаны данные учетной записи, под которой она запускается, вам нужно открыть задачу и ввести пароль еще раз после завершения импорта.

Если импорт завершился с ошибкой, вы можете выполнить одно из следующих действий:

- Для переноса данных с поддержкой иерархии Сервера администрирования вы можете импортировать файл экспорта еще раз.
- Для переноса данных без поддержки иерархии Сервера администрирования вы можете запустить мастер переноса данных, чтобы выбрать другой файл экспорта, а затем импортировать его снова.

Вы можете проверить, были ли объекты группы, входящие в область экспорта, успешно импортированы в Kaspersky Security Center Linux. Для этого перейдите в раздел **Активы (Устройства)** и убедитесь, что импортированные объекты отображаются в соответствующих подразделах.

Обратите внимание, что импортированные управляемые устройства отображаются в подразделе **Управляемые устройства**, но они не видны в сети и на них не установлен и не запущен Агент администрирования (значение *Нет* в столбцах **Видимо в сети**, **Агент администрирования установлен**, **Агент администрирования запущен**).

Для завершения переноса данных вам необходимо переключить управляемые устройства под управление Kaspersky Security Center Linux.

Переключение управляемых устройств под управление Kaspersky Security Center Linux

После успешного импорта информации об управляемых устройствах, объектах и их параметрах в Kaspersky Security Center Linux для завершения переноса данных вам необходимо переключить управляемые устройства под управление Kaspersky Security Center Linux.

Вы можете переместить управляемые устройства под управление Kaspersky Security Center Linux одним из следующих способов:

- Используя утилиту klmover.
- Используя задачу *Смена Сервера* администрирования.
- Восстановив сертификат и закрытый ключ Сервера администрирования из резервной копии (только для переноса данных в Kaspersky Security Center Linux 15.1 и выше).

  Подробнее см. шаг 6 основного сценария переноса данных.
- Установив Агент администрирования на управляемые устройства с помощью задачи удаленной установки.

Чтобы переключить управляемые устройства под управление Kaspersky Security Center Linux, установив Агент администрирования:

1. Удалите Агент администрирования на импортированных управляемых устройствах, которые будут переключены под управление Kaspersky Security Center Linux.
2. Переключитесь на Сервер администрирования Kaspersky Security Center Windows.
3. Перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты** и откройте свойства существующего инсталляционного пакета Агента администрирования.

   Если инсталляционный пакет Агента администрирования отсутствует в списке пакетов, загрузите новый.

   Вы также можете создать и использовать автономный инсталляционный пакет для локальной установки Агента администрирования.

4. На вкладке **Параметры** выберите раздел **Подключение**. Укажите параметры подключения Сервера администрирования Kaspersky Security Center Linux.

5. Создайте задачу удаленной установки для импортированных управляемых устройств, а затем укажите перенастроенный инсталляционный пакет Агента администрирования.

   Вы можете установить Агент администрирования с помощью Сервера администрирования Kaspersky Security Center Windows или с помощью устройства под управлением Windows, которое выполняет роль точки распространения. Если вы используете Сервер администрирования, включите параметр **Средствами операционной системы с помощью Сервера администрирования**. Если вы используете точку распространения, включите параметр **Средствами операционной системы с помощью точек распространения**.

6. Запустите задачу удаленной установки приложения.

После успешного завершения задачи удаленной установки перейдите на Сервер администрирования Kaspersky Security Center Linux и убедитесь, что управляемые устройства видны в сети и что на них установлен и запущен Агент администрирования (значение *Да* в столбцах **Видимо в сети**, **Агент администрирования установлен** и **Агент администрирования запущен**).

Вход в приложение Kaspersky Security Center Web Console и выход из него

Вы можете войти в Kaspersky Security Center Web Console после установки Сервера администрирования и Сервера Web Console. Вам нужно знать веб-адрес Сервера администрирования и номер порта, указанный во время установки (по умолчанию используется порт 8080). В вашем браузере JavaScript должен быть включен.

Вы можете войти в Kaspersky Security Center Web Console следующими способами:

- Используя доменную аутентификацию.

  Если вы выберете этот способ, убедитесь, что опрос контроллеров домена активирован и доменные пользователи добавлены на Сервер администрирования.

- Указав имя доменного пользователя и пароль.

- Указав имя учетной записи и пароль администратора.

Учетной записи пользователя, под которой вы хотите войти в Kaspersky Security Center Web Console, должна быть назначена роль. Прежде чем войти в приложение убедитесь, что доменной учетной записи или внутренней учетной записи пользователя назначена роль. Иначе возникнет ошибка.

Вход с использованием доменной аутентификации

Чтобы войти в Kaspersky Security Center Web Console, используя доменную аутентификацию:

1. В вашем браузере перейдите https://<адрес Kaspersky Security Center Web Console>:<Номер порта>

   Отобразится страница входа в приложение.

2. Если вы добавили несколько доверенных серверов администрирования, в списке выберите Сервер администрирования, к которому вы хотите подключиться.

   Если вы добавили только один Сервер администрирования, список Серверов администрирования не отображается.

3. Выполните одно из следующих действий:

   - Нажмите на кнопку **Использовать доменную аутентификацию**.
   - Если на Сервере создан один или несколько виртуальных Серверов администрирования и вы хотите войти на виртуальный Сервер с использованием доменной аутентификации:

     a. Нажмите на кнопку **Показать параметры виртуального Сервера**.

     b. Введите имя виртуального Сервера администрирования, которое вы указали при создании виртуального Сервера.

     c. Нажмите на кнопку **Использовать доменную аутентификацию**.

4. Если для вашей учетной записи включена двухфакторная аутентификация, укажите код безопасности, сгенерированный приложением для аутентификации на мобильном устройстве.

   При необходимости вы можете вернуться на страницу входа.

После входа в систему информационная панель отображается с языком и темой, которые вы использовали в последний раз. Вы можете перемещаться по Kaspersky Security Center Web Console и использовать ее для работы с Kaspersky Security Center.

Вход с указанием имени учетной записи и пароля администратора

Чтобы войти в Kaspersky Security Center Web Console, указав имя учетной записи и пароль администратора:

1. В вашем браузере перейдите https://<адрес Kaspersky Security Center Web Console>:<Номер порта>

   Отобразится страница входа в приложение.

2. Если вы добавили несколько доверенных серверов администрирования, в списке выберите Сервер администрирования, к которому вы хотите подключиться.

   Если вы добавили только один Сервер администрирования, список Серверов администрирования не отображается.

3. Выполните одно из следующих действий:

   - Чтобы войти на Сервер администрирования с доменной учетной записью пользователя:

     a. Введите имя пользователя и пароль доменного пользователя.

Вы можете ввести имя доменного пользователя в одном из следующих форматов:

- `Username@dns.domain`.
- `NTDOMAIN\Username`

b. Нажмите на кнопку **Войти**.

Прежде чем войти в систему с доменной учетной записью пользователя, опросите контроллеры домена, чтобы получить список пользователей домена.

- Для входа на Сервер администрирования:

  a. Введите имя пользователя и пароль локального администратора.

  b. Нажмите на кнопку **Войти**.

- Если на Сервере создан один или несколько виртуальных Серверов администрирования и вы хотите войти на виртуальный Сервер:

  a. Нажмите на кнопку **Показать параметры виртуального Сервера**.

  b. Введите имя виртуального Сервера администрирования, которое вы указали при создании виртуального Сервера.

  c. Введите имя пользователя и пароль администратора, имеющего права на виртуальном Сервере администрирования.

  d. Нажмите на кнопку **Войти**.

4. Если для вашей учетной записи включена двухфакторная аутентификация, укажите код безопасности, сгенерированный приложением для аутентификации на мобильном устройстве.

   При необходимости вы можете вернуться на страницу входа.

5. Если для вашей учетной записи включено принудительное изменение пароля или срок действия пароля истек, отобразится окно изменения пароля. Установите новый пароль для входа в Kaspersky Security Center Web Console.

После входа в систему информационная панель отображается с языком и темой, которые вы использовали в последний раз. Вы можете перемещаться по Kaspersky Security Center Web Console и использовать ее для работы с Kaspersky Security Center.

Выход

Чтобы выйти из Kaspersky Security Center Web Console,

в главном меню перейдите в параметры своей учетной записи и выберите **Выход.**

Приложение Kaspersky Security Center Web Console закрыто, отображается страница входа в приложение.

Identity and Access Manager в Kaspersky Security Center Web Console

В этом разделе представлена информация о Identity and Access Manager (далее также IAM).

О компоненте Identity and Access Manager

Identity and Access Manager (далее также IAM) – это компонент Kaspersky Security Center Web Console, позволяющий использовать единый вход (Single Sign-on, SSO) между Kaspersky Security Center Web Console и веб-интерфейсом Kaspersky Industrial CyberSecurity for Networks. IAM использует протокол OAuth 2.0 для авторизации Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center Web Console.

В этом случае приложение Kaspersky Industrial CyberSecurity for Networks, доступ к которому вы получаете через Kaspersky Security Center Web Console, называется *сервером ресурсов*, Kaspersky Security Center Web Console и веб-интерфейс Kaspersky Industrial CyberSecurity for Networks называются *клиенты OAuth 2.0*. Сервер ресурсов – это приложение, которое работает с несколькими пользователями и требует авторизации. Клиент использует *токен* для авторизации на сервере ресурсов. Токен – это уникальная последовательность байтов. По истечении срока действия токена он автоматически перевыпускается. IAM действует как единый сервер авторизации для нескольких клиентов OAuth 2.0.

Вы можете установить IAM при установке Kaspersky Security Center Web Console. Вы можете включить его позже в любой момент в параметрах Kaspersky Security Center Web Console. Если Сервер Kaspersky Industrial CyberSecurity или веб-интерфейс Kaspersky Industrial CyberSecurity установлены на устройстве, управляемым тем же Сервером администрирования, IAM обнаруживает это приложение, и в Kaspersky Security Center Web Console отображается уведомление об этом. Вы можете зарегистрировать Kaspersky Industrial CyberSecurity for Networks, а затем использовать SSO как для Kaspersky Security Center Web Console, так и для веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

Если вы выйдете из Kaspersky Security Center Web Console, ваш сеанс в веб-интерфейсе Kaspersky Industrial CyberSecurity for Networks завершится, и вам придется снова войти в Kaspersky Security Center Web Console.

Включение Identity and Access Manager: сценарий

Предварительные требования

Перед началом работы убедитесь, что у вас есть доступ к Kaspersky Industrial CyberSecurity for Networks версии 3.1 или новее.

Этапы

Включение Identity and Access Manager (также называемого IAM) происходит поэтапно:

1. **Проверка необходимых портов**

   Убедитесь, что на устройстве, на котором установлено приложение Kaspersky Security Center Web Console, открыты порты 3333, 4004 и 4444. Эти порты необходимы для использования OAuth 2.0. Вы можете изменить номера портов по умолчанию в окне параметров Kaspersky Security Center Web Console.

   Кроме портов 3333, 4004 и 4444, Kaspersky Security Center Web Console также использует порты 4445, 2444 и 2445 для различных целей.

2. **Установка Identity and Access Manager**

   Во время установки Kaspersky Security Center Web Console укажите, что вы хотите установить Identity and Access Manager. Если вы этого не сделали, запустите еще раз мастер установки Kaspersky Security Center Web Console.

3. **Настройка Identity and Access Manager**

   В окне параметров Kaspersky Security Center Web Console убедитесь, что переключатель **Identity and Access Manager (IAM)** включен. Также укажите DNS-имя устройства, на котором установлено приложение Kaspersky Security Center Web Console: клиентские приложения будут подключаться к этому устройству.

4. **Указание параметров токена**

   В окне параметров Kaspersky Security Center Web Console укажите время жизни токенов и время ожидания авторизации, которые будет использовать Identity and Access Manager. Вы можете использовать значения по умолчанию или указать свои значения в соответствии с вашими требованиями.

5. **Предоставление сертификатов**

   Если вы предпочитаете использовать сертификаты, сгенерированные Сервером администрирования, то в окне параметров Kaspersky Security Center Web Console загрузите корневые сертификаты для портов, используемых IAM, и раздайте их рабочим станциям пользователей Kaspersky Security Center Web Console. В противном случае браузеры пользователей будут отображать сообщения об ошибках при попытке подключения к Kaspersky Security Center Web Console.

6. **Регистрация Серверов Kaspersky Industrial CyberSecurity for Networks и веб-интерфейсов Kaspersky Industrial CyberSecurity for Networks**

   При установке IAM в Kaspersky Security Center Web Console отображается сообщение о том, что Сервер Industrial CyberSecurity for Networks (или несколько Серверов) и один или несколько веб-интерфейсов Kaspersky Industrial CyberSecurity for Networks ожидают регистрации. Нажмите на это сообщение, чтобы зарегистрировать Сервер Kaspersky Industrial CyberSecurity for Networks Server (или Серверы) и веб-интерфейс (или веб-интерфейсы).

Результаты

После завершения этого сценария вы сможете использовать SSO и IAM для Kaspersky Industrial CyberSecurity for Networks и Kaspersky Security Center Web Console.

Настройка Identity and Access Manager в Kaspersky Security Center Web Console

Чтобы настроить Identity and Access Manager в соответствии с вашими требованиями:

1. В главном меню перейдите в раздел **Параметры** → **Identity and Access Manager**.
2. В разделе **Identity and Access Manager** убедитесь, что Identity and Access Manager включен.
3. Перейдите по ссылке **Параметры** в блоке **Сетевое имя устройства Identity and Access Manager**.
4. Укажите DNS-имя устройства, на котором вы установили Identity and Access Manager. Клиентские приложения будут подключаться к этому устройству.
5. Если хотите, измените параметры токена по умолчанию, параметры сертификата, а также номера портов нажав на ссылку **Параметры** под соответствующей группой параметров.

Identity and Access Manager включен и работает в соответствии с вашими требованиями.

Регистрация приложения Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center Web Console

Чтобы начать работу с приложением Kaspersky Industrial CyberSecurity for Networks через Kaspersky Security Center Web Console, необходимо предварительно зарегистрировать его в Kaspersky Security Center Web Console.

Чтобы зарегистрировать приложение Kaspersky Industrial CyberSecurity for Networks:

1. Убедитесь, что сделано следующее:
   - Вы загрузили и установили веб-плагин Kaspersky Industrial CyberSecurity for Networks.

     Также можно сделать это позже, ожидая синхронизацию Сервера Kaspersky Industrial CyberSecurity for Networks с Сервером администрирования.
   - Вы завершили сценарий подготовки к использованию технологии единого входа (SSO).
   - Необходимые параметры в веб-интерфейсе Kaspersky Industrial CyberSecurity for Networks заданы на странице Kaspersky Security Center. Подробную информацию см. в справке Kaspersky Industrial CyberSecurity for Networks.
   - Вы вошли в Kaspersky Security Center Web Console под учетной записью администратора.
   - IAM настроен.

2. Переместите устройство, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks, из группы Нераспределенные устройства в группу Управляемые устройства:

   a. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.

   b. Установите флажок рядом с устройством, на котором установлен Kaspersky Industrial CyberSecurity for Networks Server.

   c. Нажмите на кнопку **Переместить в группу**.

   d. В иерархии групп администрирования установите флажок рядом с группой Управляемые устройства.

   e. Нажмите на кнопку **Переместить**.

3. Перейдите к свойствам устройства, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks.

4. На странице свойств устройства в разделе **Общие**, выберите параметр **Не разрывать соединение с Сервером администрирования**, а затем нажмите на кнопку **Сохранить**.

5. В окне свойств устройства выберите раздел **Приложения**.

6. В разделе **Приложения** выберите Агент администрирования.

7. Если текущий статус приложения *Остановлено*, подождите, пока он не изменится на *Выполняется*.

   Это может занять до 15 минут. Если вы еще не установили веб-плагин Kaspersky Industrial CyberSecurity for Networks, вы можете сделать это сейчас, пока ждете.

8. В главном меню перейдите в раздел **Параметры** → **Identity and Access Manager**.

   В поле **Запросы на регистрацию**, отображается один ожидающий запрос.

9. Перейдите по ссылке **Параметры**, расположенной ниже поля **Запросы на регистрацию**.

10. В открывшемся списке зарегистрированных клиентов установите флажок рядом с названием того Сервера Kaspersky Industrial CyberSecurity for Networks, который имеет статус *Ожидает*, а затем нажмите на кнопку **Одобрить**.

    Если вы не хотите регистрировать Сервер Kaspersky Industrial CyberSecurity for Networks, вы можете нажать на кнопку Отклонить и вернуться к этому списку позже.

    После того, как вы нажмете на кнопку **Одобрить**, статус меняется на *Одобрено*, а затем на *Готов*. Если статус не поменялся, вы можете нажать на кнопку Обновить.

11. Закройте список зарегистрированных клиентов и убедитесь, что значение в поле **Зарегистрированные клиенты** увеличилось.

12. Чтобы добавить виджет Kaspersky Industrial CyberSecurity for Networks на панель управления:

    a. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.

    b. В панели управления нажмите на кнопку **Добавить или восстановить веб-виджет**.

    c. В появившемся виджете нажмите на кнопку **Другое**.

    d. Выберите виджет Kaspersky Industrial CyberSecurity for Networks.

Теперь вы можете перейти в веб-интерфейс Kaspersky Industrial CyberSecurity for Networks по ссылке в виджете.

После завершения процедуры регистрации появится новая кнопка **Kaspersky Security Center**, которая отображается на странице входа в веб-интерфейс Kaspersky Industrial CyberSecurity for Networks. Вы можете нажать на эту кнопку, чтобы войти в веб-интерфейс Kaspersky Industrial CyberSecurity for Networks под своими учетными данными Kaspersky Security Center.

Время жизни токенов и время ожидания авторизации для Identity and Access Manager

При настройке компонента Identity and Access Manager (далее также IAM) необходимо указать параметры времени жизни токена и время ожидания авторизации. Параметры по умолчанию разработаны с учетом одновременно и стандартов безопасности, и нагрузки на Сервер. Вы можете менять эти параметры в соответствии с политиками вашей организации.

IAM автоматически повторно выпускает токен, когда срок его действия истекает.

В таблице ниже перечислены параметры времени жизни токена по умолчанию.

Параметры времени жизни токена

Токен	Время жизни по умолчанию (в секундах)	Описание
Идентификационный токен (id_token)	86400	Идентификационный токен, используемый клиентом OAuth 2.0 (то есть Kaspersky Security Center Web Console или веб-интерфейсом Kaspersky Industrial CyberSecurity). IAM отправляет идентификатор токена, который содержит информацию о пользователе (то есть профиль пользователя) клиенту.
Токен доступа (access_token)	86400	Токен доступа, используемый клиентом OAuth 2.0 для доступа к серверу ресурсов от имени владельца ресурса, определенного IAM.
Обновить токен (refresh_token)	172800	Клиент OAuth 2.0 использует этот токен для повторной выдачи идентификационного токена и токена доступа.

В таблице ниже приведено время ожидания для auth_code и login_consent_request.

Параметры времени ожидания авторизации

Параметр	Время ожидания по умолчанию (в секундах)	Описание
Код авторизации (auth_code)	3600	Время ожидания обмена кода токена. Клиент OAuth 2.0 отправляет этот код на сервер ресурсов и взамен получает токен доступа.
Время ожидания запроса на вход (login_consent_request)	3600	Время ожидания для делегирования прав пользователя клиенту OAuth 2.0.

Для получения дополнительной информации о токенах см. веб-сайт OAuth.

Чтобы настроить время ожидания для клиентов, у которых не обнаружена активность мыши или клавиатуры:

1. В папке установки Kaspersky Security Center Web Console найдите и откройте файл config.json. Файл содержит параметры для настройки времени ожидания бездействия клиентов.

2. Используйте параметр `clientIdleTimeout`, чтобы указать время в миллисекундах, по истечении которого неактивному клиенту отобразится всплывающее окно с предупреждением.

3. Используйте параметр `clientLogoutTimeout`, чтобы указать время в миллисекундах, по истечении которого IAM-авторизация для неактивного клиента завершается. Значение параметра `ClientLogoutTimeout` отсчитывается последовательно после параметра `clientIdleTimeout`.

Загрузка и распространение IAM-сертификатов

По умолчанию Identity and Access Manager использует сертификаты, созданные Сервером администрирования, для предоставления доступа браузерам к Kaspersky Security Center Web Console. Вы также можете использовать пользовательские сертификаты. Какой бы сертификат вы ни использовали, вам нужно убедиться, что все рабочие станции, с которых пользователи Kaspersky Security Center Web Console обращаются к Kaspersky Security Center Web Console, доверяют этому сертификату.

Чтобы загрузить и распространить сертификаты:

1. В главном меню перейдите в раздел **Параметры → Identity and Access Manager**.

2. Для каждого сертификата нажмите на ссылку **Настройки** под соответствующей группой параметров, и выполните одно из следующих действий:

   - Если вы хотите использовать сертификат, сгенерированный Сервером администрирования при установке Kaspersky Security Center Web Console:

     1. Выберите **Сертификат, созданный Сервером администрирования** в открывшемся окне свойств сертификата.

     2. Нажмите на кнопку **Загрузить**, чтобы загрузить сертификат.

     3. Распространите загруженный сертификат на все рабочие станции, с которых пользователи Kaspersky Security Center Web Console получают доступ к Kaspersky Security Center Web Console.

   - Если у вас есть сертификат, который вы хотите использовать:

     1. Выберите **Пользовательский TLS-сертификат** в открывшемся окне свойств сертификата.

     2. Выберите файл сертификата и закрытый ключ.

     3. Нажмите на кнопку **OK**.

     4. Распространите сертификат на все рабочие станции, с которых пользователи получают доступ к Kaspersky Security Center Web Console или веб-интерфейсу Kaspersky Industrial CyberSecurity.

Сертификаты предоставляют пользователям доступ к Kaspersky Security Center Web Console и веб-интерфейсу Kaspersky Industrial CyberSecurity.

Вам необходимо своевременно перевыпустить все сертификаты. Сертификаты, сгенерированные Сервером администрирования, необходимо заново сгенерировать вручную. Сертификаты, сгенерированные установщиком Kaspersky Security Center Web Console, необходимо повторно сгенерировать с помощью установщика.

Отключение Identity and Access Manager

Вы можете выключить Identity and Access Manager (IAM).

Чтобы отключить IAM,

1. В главном меню перейдите в раздел **Параметры** → **Интеграция**.
2. В разделе **Identity and Access Manager** установите переключатель **Identity and Access Manager** в положение выключено.

Вы можете включить IAM позже в любое время.

Если вы обновите Kaspersky Security Center Web Console через установщик и укажете, что вы не хотите устанавливать IAM, то Kaspersky Security Center Web Console будет обновлен, а IAM не будет установлен. С вашего устройства будут удалены: вся информация об интеграции с Kaspersky Industrial CyberSecurity for Networks, файлы конфигурации IAM и файлы журналов событий.

Настройка доменной аутентификации с использованием протоколов NTLM и Kerberos

Kaspersky Security Center 15.1 позволяет использовать доменную аутентификацию в OpenAPI по протоколам NTLM и Kerberos. Использование доменной аутентификации позволяет пользователю Windows включить безопасную аутентификацию в Kaspersky Security Center Web Console без повторного ввода пароля в корпоративной сети (единый вход).

Доменная аутентификация в OpenAPI по протоколу Kerberos имеет следующие ограничения:

- Пользователь Kaspersky Security Center Web Console должен пройти аутентификацию в Active Directory по протоколу Kerberos. У пользователя должен быть действующий мандат на выдачу мандатов Kerberos (далее также TGT). TGT выдается автоматически при аутентификации в домене.
- Вам нужно настроить аутентификацию Kerberos в браузере. Подробнее см. в документации используемого вами браузера.

Если вы хотите использовать доменную аутентификацию с использованием протоколов Kerberos, ваша сеть должна соответствовать следующим условиям:

- Сервер администрирования должен запускаться под доменной учетной записью.
- Сервер Kaspersky Security Center Web Console установлен на том же устройстве, что и Сервер администрирования.

- Для учетной записи Сервера администрирования необходимо указать следующие имена субъектов службы (SPN):

  - "http/<server.fqnd.name>"

  - "http/<server>"

  Здесь <server> – сетевое имя устройства Сервера администрирования, <server.fqnd.name> – полное доменное имя устройства Сервера администрирования.

- При подключении через Консоль администрирования или Kaspersky Security Center Web Console необходимо указывать адрес Сервера администрирования точно так же, как адрес, для которого зарегистрировано имя субъекта-службы (SPN). Вы можете указать или <server.fqnd.name> или <server>.

- Для входа без пароля процесс браузера, в котором открыта Kaspersky Security Center Web Console, должен работать под доменной учетной записью.

Протоколы Kerberos и NTLM поддерживаются только в OpenAPI для Kaspersky Security Center 15.1. Эти протоколы не поддерживаются в OpenAPI для Kaspersky Security Center Linux.

Настройка Сервера администрирования

В этом разделе описан процесс настройки и свойства Сервера администрирования.

Настройка подключения Kaspersky Security Center Web Console к Серверу администрирования

Чтобы задать порты подключения к Серверу администрирования:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Порты подключения**.

Будут отображены основные параметры подключения к выбранному Серверу Администрирования.

Приложение Kaspersky Security Center Web Console подключено к Серверу администрирования по SSL-порту TCP 13299. Этот же порт может использоваться объектами автоматизации klakaut.

Порт TCP 14000 может использоваться для подключения Kaspersky Security Center Web Console, точек распространения, подчиненных Серверов администрирования и объектов автоматизации утилиты klakaut, а также для получения данных с клиентских устройств.

Как правило, SSL-порт TCP 13000 могут использовать только Агент администрирования, подчиненный Сервер и главный Сервер администрирования, размещенный в демилитаризованной зоне. В некоторых случаях может быть необходимо подключение Kaspersky Security Center Web Console по SSL-порту 13000:

- если предпочтительно использовать один и тот же SSL-порт как для Kaspersky Security Center Web Console, так и для других активностей (для получения данных с клиентских устройств, подключения точек распространения, подключения подчиненных Серверов администрирования);
- если объект автоматизации утилиты klakaut подключается к Серверу администрирования не напрямую, а через точку распространения, размещенную в демилитаризованной зоне.

Настройка журнала событий подключения к Серверу администрирования

Можно сохранить в файл журнала историю подключений и попыток подключения к Серверу администрирования в процессе его работы. Информация в файле позволит отследить не только подключения внутри инфраструктуры сети, но и попытки несанкционированного доступа к серверам.

Чтобы настроить регистрацию событий подключения к Серверу администрирования:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Порты подключения**.

3. Включите параметр **Записывать события соединения с Сервером администрирования в журнал**.

Все последующие события входящих подключений к Серверу администрирования, результаты аутентификации и ошибки SSL будут записываться в файл %ProgramData%\KasperskyLab\adminkit\logs\SC.syslog.

Настройка параметров доступа Сервера администрирования к интернету

Доступ к интернету необходимо настроить, чтобы использовать Kaspersky Security Network и загружать обновления антивирусных баз для Kaspersky Security Center и управляемых приложений "Лаборатории Касперского".

Чтобы указать параметры доступа Сервера администрирования к интернету:

1. В главном меню нажмите на значок параметров ( ) рядом с именем Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры доступа к сети интернет**.

3. Включите параметр **Использовать прокси-сервер**, если требуется использовать прокси-сервер для подключения к интернету. Если параметр включен, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

   - **Адрес**

     Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.

   - **Номер порта**

     Номер порта, через который будет установлено прокси-подключение Kaspersky Security Center.

   - **Не использовать прокси-сервер для локальных адресов**

     При подключении к устройствам в локальной сети не будет использоваться прокси-сервер.

   - **Аутентификация на прокси-сервере**

     Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

     Поле ввода доступно, если установлен флажок **Использовать прокси-сервер**.

   - **Имя пользователя**

     Учетная запись пользователя, от имени которого будет выполняться подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

   - **Пароль**

     Пароль пользователя, с помощью учетной записи которого выполняется подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

     Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

Также можно настроить доступ в интернет с помощью мастера первоначальной настройки.

Настройка количества событий в хранилище событий

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, приложение вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400 000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Приложение проверяет базу данных каждые 10 минут. Если количество событий достигает на 10 000 больше указанного максимального значения, приложение удаляет самые старые события, чтобы осталось только указанное максимальное количество событий.

Когда Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий Kaspersky Event Log. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления.

Чтобы ограничить количество событий, которые можно сохранить в хранилище событий на Сервере администрирования:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Хранилище событий**. Укажите максимальное количество событий, хранящихся в базе данных.

3. Нажмите на кнопку **Сохранить**.

Также вы можете выполнить следующее:

- Изменить параметры любой задачи, чтобы сохранять события, связанные с ходом выполнения задачи, или сохранять только результаты выполнения задачи.

- Уменьшить или выключить период хранения для событий Сервера администрирования, Агента администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах.

Таким образом вы уменьшаете количество событий в базе данных, увеличиваете скорость работы сценариев, связанных с анализом таблицы событий в базе данных, и снижаете риск вытеснения критических событий большим количеством событий.

Параметры подключения устройств с защитой на уровне UEFI

Устройство с защитой на уровне UEFI – это устройство со встроенным на уровне BIOS решением или приложением "Лаборатории 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 безопасности. Kaspersky Security Center поддерживает управление такими устройствами.

Чтобы изменить параметры подключения устройств с защитой на уровне UEFI:

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 **Дополнительные порты**.

3. Измените требуемые параметры:

   - **Открыть порт для устройств с защитой на уровне UEFI и устройств с KasperskyOS**

     Если флажок установлен, то устройства с защитой на уровне UEFI могут подключаться к Серверу администрирования.

     По умолчанию флажок установлен.

- **Порт для устройств с защитой на уровне UEFI и устройств с KasperskyOS**

  Вы можете изменить номер порта, если установлен флажок **Открыть порт для устройств с защитой на уровне UEFI**. По умолчанию используется порт 13294.

4. Нажмите на кнопку **Сохранить**.

Устройства с защитой на уровне UEFI могут подключаться к Серверу администрирования.

Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования

Добавление подчиненного Сервера администрирования (выполняется с будущим главным Сервером администрирования)

Вы можете добавить Сервер администрирования в качестве подчиненного Сервера, установив таким образом отношение иерархии "главный Сервер – подчиненный Сервер".

Чтобы добавить Сервер администрирования, доступный для подключения через Kaspersky Security Center Web Console, в качестве подчиненного Сервера:

1. Убедитесь, что порт 13000 будущего главного Сервера доступен для приема подключений от подчиненных Серверов администрирования.

2. На будущем главном Сервере администрирования нажмите на значок параметров ( ).

3. На открывшейся странице свойств перейдите на вкладку **Серверы администрирования**.

4. Установите флажок рядом с именем группы администрирования, в которую вы хотите добавить Сервер администрирования.

5. В меню выберите пункт **Подключить подчиненный Сервер администрирования**.

   Запустится мастер добавления подчиненного Сервера администрирования. Для продолжения работы мастера нажмите на кнопку **Далее**.

6. Заполните следующие поля:

   - **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**

     Выберите этот параметр, если подчиненный Сервер администрирования находится в демилитаризованной зоне (DMZ).

     Если выбран этот параметр, необходимо указать **Адрес подчиненного Сервера**.

     Если выбран этот параметр, главный Сервер администрирования инициирует подключение к подчиненному Серверу администрирования. Иначе подчиненный Сервер администрирования инициирует подключение к главному Серверу администрирования.

   - **Имя подчиненного Сервера администрирования**

     Имя подчиненного Сервера администрирования, которое будет отображаться в иерархии Серверов. Вы можете ввести IP-адрес в качестве имени или использовать такое имя, как, например, "Подчиненный Сервер для группы 1".

- **Адрес подчиненного Сервера администрирования (необязательно)**

  Укажите IP-адрес или доменное имя подчиненного Сервера администрирования.

  Этот параметр необходим, если включен параметр **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.

- **SSL-порт Сервера администрирования**

  После построения иерархии укажите номер SSL-порта, который будет использоваться для взаимодействия между главным Сервером администрирования и подчиненным Сервером администрирования. По умолчанию установлен порт 13000.

- **API-порт Сервера администрирования**

  Номер порта, который Web Console будет использовать для приема подключений от подчиненного Сервера администрирования по OpenAPI. По умолчанию установлен порт 13299.

  При построении иерархии Web Console подключается к будущему подчиненному Серверу, запрашивает учетные данные, получает открытый сертификат и выполняет первоначальную настройку.

  После построения иерархии Сервера администрирования порт 13299 больше не будет использоваться. Серверы администрирования будут взаимодействовать через порт 13000.

7. Укажите сертификат подчиненного Сервера администрирования. Если вы указали параметр **Адрес подчиненного Сервера**, чтобы получить сертификат, нажмите на кнопку **Получить с подчиненного Сервера администрирования**. Или нажмите на кнопку **Выбрать файл сертификата** и найдите файл сертификата.

8. Задайте параметры подключения:

   - Введите адрес будущего главного Сервера администрирования.

   - Если будущий подчиненный Сервер администрирования использует прокси-сервер, введите адрес прокси-сервера и учетные данные пользователя для подключения к прокси-серверу.

9. Введите учетные данные пользователя, имеющего права доступа на будущий подчиненный Сервер администрирования.

10. Если двухфакторная аутентификация включена и настроена, укажите код безопасности, сгенерированный приложением для аутентификации.

    Если двухфакторная аутентификация включена, но не настроена для учетной записи, которую вы указали, создайте иерархию только из будущего подчиненного Сервера (см. инструкции ниже).

Если параметры соединения верны, устанавливается соединение с будущим подчиненным Сервером и строится иерархия "главный/подчиненный". Если подключение не удалось, проверьте параметры подключения или укажите сертификат будущего подчиненного Сервера вручную.

Соединение между главным и подчиненным Серверами администрирования устанавливается через порт 13000. Задачи и политики главного Сервера администрирования получены и применены. Подчиненный Сервер администрирования отображается на главном Сервере администрирования, в группе администрирования, в которую он был добавлен.

Добавление подчиненного Сервера администрирования (выполняется с будущим подчиненным Сервером администрирования)

Если вы не можете подключится к будущему подчиненному Серверу администрирования (например, потому что он был временно отключен или недоступен), вы все равно можете добавить подчиненный Сервер администрирования.

Чтобы добавить Сервер администрирования, недоступный для подключения через Kaspersky Security Center Web Console, в качестве подчиненного Сервера:

1. Отправьте файл сертификата будущего главного Сервера администрирования системному администратору офиса, в котором находится будущий подчиненный Сервер администрирования. (Например, вы можете записать файл на внешнее устройство или отправить его по электронной почте.)

   Файл сертификата находится на будущем главном Сервере администрирования по адресу %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

2. Предложите системному администратору, ответственному за будущий подчиненный Сервер администрирования, следующее:

   a. Нажмите на значок параметров ( ).

   b. На открывшейся странице свойств перейти в раздел **Иерархия Серверов администрирования** на вкладке **Общие**.

   c. Выберите параметр **Данный Сервер администрирования является подчиненным в иерархии**.

   d. В поле **Адрес главного Сервера администрирования** введите сетевое имя будущего главного Сервера администрирования.

   e. Выбрать ранее сохраненный файл сертификата будущего главного Сервера, нажав на кнопку **Обзор**.

   f. Если необходимо, установить флажок **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.

   g. Если подключение к будущему подчиненному Серверу администрирования выполняется с помощью прокси-сервера, выберите параметр **Использовать прокси-сервер** и задайте параметры подключения.

   h. Нажмите на кнопку **Сохранить**.

Отношение "Главный Сервер – подчиненный Сервер" будет установлено. Главный Сервер начинает принимать подключение от подчиненного Сервера, используя порт 13000. Задачи и политики главного Сервера администрирования получены и применены. Подчиненный Сервер администрирования отображается на главном Сервере администрирования, в группе администрирования, в которую он был добавлен.

В главном меню нажмите на значок параметров ( ) рядом с именем Сервера администрирования.

Просмотр списка подчиненных Серверов администрирования

Чтобы просмотреть список подчиненных (включая виртуальные) Серверов администрирования:

В главном меню нажмите на имя Сервера администрирования, которое находится рядом со значком параметров ().

Отобразится раскрывающийся список подчиненных (включая виртуальные) Серверов администрирования.

Вы можете перейти на любой из этих Серверов администрирования, нажав на его имя.

Группы администрирования тоже отображаются, но они неактивны и недоступны для управления в этом меню.

Если вы подключены к главному Серверу администрирования в Kaspersky Security Center Web Console и не можете подключиться к виртуальному Серверу администрирования, управляемому подчиненным Сервером администрирования, вы можете воспользоваться одним из следующих способов:

- **Измените существующую установку Kaspersky Security Center Web Console, добавив подчиненный Сервер в список доверенных Серверов администрирования**. После этого вы сможете подключиться к виртуальному Серверу администрирования в Kaspersky Security Center Web Console.

  1. Запустите на устройстве, на котором установлено приложение Kaspersky Security Center Web Console, исполняемый файл ksc-web-console-<номер версии>.<номер сборки>.exe под учетной записью с правами администратора.

     Запустится мастер установки приложения. Для продолжения работы мастера нажмите на кнопку **Далее**.

  2. Выберите параметр **Обновить**.

  3. На странице **Тип изменения** выберите параметр **Изменить параметры подключения**.

  4. На шаге **Доверенные Серверы администрирования** добавьте требуемый подчиненный Сервер администрирования.

  5. На последнем шаге нажмите на кнопку **Изменить**, чтобы применить новые параметры.

  6. После успешного завершения настройки приложения нажмите на кнопку **Готово**.

- Используйте Kaspersky Security Center Web Console, чтобы напрямую подключиться к подчиненному Серверу администрирования, на котором был создан виртуальный Сервер. После этого вы сможете переключиться на виртуальный Сервер администрирования в Kaspersky Security Center Web Console.

- Используйте Консоль администрирования на основе MMC для прямого подключения к виртуальному Серверу.

Удаление иерархии Серверов администрирования

Если вам больше не нужна иерархия Серверов администрирования, вы можете отключить их от этой иерархии.

Чтобы удалить иерархию Серверов администрирования:

1. В главном меню нажмите на значок параметров ( ) рядом с именем главного Сервера администрирования.
2. На открывшейся странице выберите 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.

Обслуживание Сервера администрирования

Обслуживание Сервера администрирования позволяет освободить место в папке Сервера администрирования и уменьшить объем базы данных за счет удаления ненужных объектов. Это поможет вам повысить производительность и надежность работы приложения. Рекомендуется обслуживать Сервер администрирования не реже раза в неделю.

Обслуживание Сервера администрирования выполняется с помощью соответствующей задачи. Во время обслуживания Сервера администрирования приложение выполняет следующие действия:

- Удаляет ненужные папки и файлы из папки хранилища.
- Удаляет ненужные записи из таблиц (также известные как "висячие указатели").
- Очищает кеш.
- Обслуживает базу данных (если вы используете SQL Server или PostgreSQL в качестве СУБД):
  - проверяет базу данных на наличие ошибок (доступно только для SQL Server);
  - перестраивает индексы базы данных;
  - обновляет статистику базы данных;
  - сжимает базу данных (если необходимо).

Задача Обслуживание Сервера администрирования создается автоматически при установке Kaspersky Security Center. Если задача Обслуживание Сервера администрирования удалена, вы можете создать ее вручную.

Чтобы создать задачу Обслуживание Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В окне мастера **Параметры новой задачи** выберите тип задачи **Обслуживание Сервера администрирования** и нажмите на кнопку **Далее**.
4. Следуйте дальнейшим шагам мастера.

В результате созданная задача отобразится в списке задач. Для одного Сервера администрирования может выполняться только одна задача Обслуживание Сервера администрирования. Если задача Обслуживание Сервера администрирования для Сервера администрирования уже создана, создание еще одной задачи Обслуживание Сервера администрирования невозможно.

Настройка интерфейса

Вы можете настроить интерфейс Kaspersky Security Center Web Console на отображение и скрытие разделов и элементов интерфейса в зависимости от используемых функций.

Чтобы настроить интерфейс Kaspersky Security Center Web Console в соответствии в соответствии с используемым в настоящее время набором функций:

1. В главном меню перейдите в параметры своей учетной записи и выберите **Параметры интерфейса.**
2. В появившемся окне **Параметры интерфейса** включите или выключите необходимые параметры.
3. Нажмите на кнопку **Сохранить**.

   После этого в консоли отображаются разделы в главном меню в соответствии с включенными параметрами. Например, если включить **Показать EDR-алерты**, раздел **Мониторинг и отчеты** → **Алерты** появится в главном меню.

Управление виртуальными Серверами администрирования

В этом разделе описываются следующие действия, как управлять виртуальными Серверами администрирования:

- создание виртуальных Серверов администрирования;
- включение и выключение виртуальных Серверов администрирования;
- назначение администратора виртуального Сервера администрирования;

- смена Сервера администрирования для клиентских устройств;
- удаление виртуальных Серверов администрирования.

Создание виртуального Сервера администрирования

Можно создать виртуальные Серверы администрирования и добавить их в группы администрирования.

При создании виртуального Сервера администрирования он наследует список пользователей и все права пользователей главного Сервера администрирования. Если пользователь имеет права доступа к главному Серверу, этот пользователь также имеет права доступа к виртуальному Серверу. После создания вы самостоятельно настраиваете права доступа к Серверам.

Чтобы создать и добавить виртуальный Сервер администрирования:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.
2. На открывшейся странице перейдите на вкладку **Серверы администрирования**.
3. Выберите группу администрирования, в которую вы хотите добавить виртуальный Сервер администрирования.
   Виртуальный Сервер администрирования будет управлять устройствами из выбранной группы (включая подгруппы).
4. В меню выберите пункт **Новый виртуальный Сервер администрирования**.
5. На открывшейся странице задайте свойства нового виртуального Сервера администрирования:
   - **Имя виртуального Сервера администрирования**.
   - **Адрес подключения Сервера администрирования**
     Вы можете указать имя или IP-адрес Сервера администрирования.
6. Из списка пользователей выберите администратора виртуального Сервера администрирования. Существующую учетную запись при необходимости можно изменить перед тем, как назначить ей роль администратора; можно также создать учетную запись.
7. Нажмите на кнопку **Сохранить**.

Новый виртуальный Сервер администрирования создан, добавлен в группу администрирования и отображается на вкладке **Серверы администрирования**.

Если вы подключены к главному Серверу администрирования в Kaspersky Security Center Web Console и не можете подключиться к виртуальному Серверу администрирования, управляемому подчиненным Сервером администрирования, вы можете воспользоваться одним из следующих способов:

- **Измените существующую установку Kaspersky Security Center Web Console, добавив подчиненный Сервер в список доверенных Серверов администрирования**. После этого вы сможете подключиться к виртуальному Серверу администрирования в Kaspersky Security Center Web Console.

  1. Запустите на устройстве, на котором установлено приложение Kaspersky Security Center Web Console, исполняемый файл ksc-web-console-<номер версии>.<номер сборки>.exe под учетной записью с правами администратора.

     Запустится мастер установки приложения. Для продолжения работы мастера нажмите на кнопку **Далее**.

  2. Выберите параметр **Обновить**.

  3. На странице **Тип изменения** выберите параметр **Изменить параметры подключения**.

  4. На шаге **Доверенные Серверы администрирования** добавьте требуемый подчиненный Сервер администрирования.

  5. На последнем шаге нажмите на кнопку **Изменить**, чтобы применить новые параметры.

  6. После успешного завершения настройки приложения нажмите на кнопку **Готово**.

- Используйте Kaspersky Security Center Web Console, чтобы напрямую подключиться к подчиненному Серверу администрирования, на котором был создан виртуальный Сервер. После этого вы сможете переключиться на виртуальный Сервер администрирования в Kaspersky Security Center Web Console.

- Используйте Консоль администрирования на основе MMC для прямого подключения к виртуальному Серверу.

Включение и выключение виртуального Сервера администрирования

Когда вы создаете виртуальный Сервер администрирования, он по умолчанию включается. Вы можете выключить или снова включить его в любое время. Выключение или включение виртуального Сервера администрирования равносильно выключению или включению физического Сервера администрирования.

Чтобы включить или выключить виртуальный Сервер администрирования:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

2. На открывшейся странице выберите вкладку **Серверы администрирования**.

3. Выберите виртуальный Сервер администрирования, который вы хотите включить или выключить.

4. В меню нажмите на кнопку **Подключить / отключить виртуальный Сервер администрирования**.

   Состояние виртуального Сервера администрирования изменяется на включено или выключено в зависимости от его предыдущего состояния. Обновленное состояние отображается рядом с именем Сервера администрирования.

Назначение администратора виртуального Сервера администрирования

Если вы используете в своей организации виртуальные Серверы администрирования, вам может потребоваться назначить отдельного администратора для каждого виртуального Сервера администрирования. Например, это может быть полезно, когда вы создаете виртуальные Серверы администрирования для управления отдельными офисами или отделами вашей организации или если вы являетесь поставщиком услуг (MSP) и управляете своими тенантами с помощью виртуальных Серверов администрирования.

При создании виртуального Сервера администрирования он наследует список пользователей и все права пользователей главного Сервера администрирования. Если пользователь имеет права доступа к главному Серверу, этот пользователь также имеет права доступа к виртуальному Серверу. После создания вы самостоятельно настраиваете права доступа к Серверам. Если вы хотите назначить администратора только для виртуального Сервера администрирования, убедитесь, что у администратора нет прав доступа на главном Сервере администрирования.

Вы назначаете администратора виртуального Сервера администрирования, предоставляя права доступа администратору к виртуальному Серверу администрирования. Вы можете предоставить требуемые права доступа одним из следующих способов:

- Настройте права доступа для администратора вручную.
- Назначьте одну или несколько пользовательских ролей администратору.

Чтобы войти в Kaspersky Security Center Web Console, администратор виртуального Сервера администрирования указывает имя виртуального Сервера администрирования, имя пользователя и пароль. Kaspersky Security Center Web Console выполняет аутентификацию администратора и открывает виртуальный Сервер администрирования, к которому у администратора есть права доступа. Администратор не может переключаться между Серверами администрирования.

Предварительные требования

Убедитесь, что выполнены следующие условия:

- Виртуальный Сервер администрирования создан.
- На главном Сервере администрирования у вас создана учетная запись для администратора, которого вы хотите назначить для виртуального Сервера администрирования.
- У вас есть право **Изменение списков управления доступом объектов** в функциональной области **Общие функции → Права пользователей**.

Настройка прав доступа вручную

Чтобы назначить администратора виртуального Сервера администрирования:

1. В главном меню переключитесь на требуемый виртуальный Сервер администрирования:

   a. Нажмите на значок шеврона (›) справа от текущего имени Сервера администрирования.

   b. Выберите требуемый Сервер администрирования.

2. В главном меню нажмите на значок параметров ( ) рядом с именем Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

3. На вкладке **Права доступа** нажмите на кнопку **Добавить**.

   Откроется единый список пользователей главного Сервера администрирования и текущего виртуального Сервера администрирования.

4. В списке пользователей выберите учетную запись администратора, которого вы хотите назначить для виртуального Сервера администрирования, и нажмите на кнопку **OK**.

   Приложение добавляет выбранного пользователя в список пользователей на вкладку **Права доступа**.

5. Установите флажок рядом с добавленной учетной записью и нажмите на кнопку **Права доступа**.

6. Настройте права администратора на виртуальном Сервере администрирования.

   Для успешной аутентификации администратор должен иметь следующие права:

   - право **Чтение** в функциональной области **Общие функции** → **Базовая функциональность**.
   - право **Чтение** в функциональной области **Общие функции** → **Виртуальные Серверы администрирования**.

Приложение сохраняет измененные права пользователя в учетной записи администратора.

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. В главном меню переключитесь на требуемый виртуальный Сервер администрирования:

   a. Нажмите на значок шеврона (›) справа от текущего имени Сервера администрирования.

   b. Выберите требуемый Сервер администрирования.

3. Назначьте новую роль или несколько ролей учетной записи администратора.

   Приложение назначает роль учетной записи администратора.

Настройка прав доступа на уровне объекта

В дополнение к назначению прав доступа на уровне функциональной области, вы можете настроить доступ к определенным объектам на виртуальном Сервере администрирования, например, к определенной группе администрирования или задаче. Для этого переключитесь на виртуальный Сервер администрирования, а затем настройте права доступа в свойствах объекта.

Смена Сервера администрирования для клиентских устройств

Вы можете сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером с помощью задачи *Смена Сервера администрирования*. После завершения задачи выбранные клиентские устройства будут под управлением указанного Сервера администрирования.

> Вы не можете использовать задачу *Смена Сервера администрирования* для клиентских устройств, подключенных к Серверу администрирования с помощью шлюзов соединения. Для таких устройств необходимо перенастроить Агент администрирования или переустановить Агент администрирования, указав шлюз соединения.

Чтобы сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге мастера **Параметры новой задачи** укажите следующие параметры:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Security Center**.

   b. В поле **Тип задачи** выберите **Смена Сервера администрирования**.

c. В поле **Название задачи** укажите название создаваемой задачи.

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 мастера **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

5. На этом шаге мастера подтвердите свое согласие с условиями смены Сервера администрирования для клиентских устройств.

6. На этом шаге мастера выберите Сервер администрирования, который вы хотите использовать для управления выбранными устройствами:

- **Смена главного Сервера администрирования**

  Чтобы переместить клиентские устройства на другой главный Сервер администрирования, укажите следующие параметры подключения к Серверу администрирования:

  1. В поле **Адрес Сервера администрирования** укажите адрес нового главного Сервера администрирования.

  2. В поле **Номер порта** укажите номер порта для подключения к Серверу администрирования.

     По умолчанию установлен порт 14000.

  3. В поле **SSL-порт** укажите номер SSL-порта главного Сервера администрирования.

     По умолчанию установлен порт 13000.

  4. При необходимости включите параметр **Использовать прокси-сервер**.

Если этот параметр выключен, для подключения устройства к Серверу администрирования используется прямое соединение.

Если этот параметр включен, укажите параметры прокси-сервера:

- **Адрес прокси-сервера**
- **Порт прокси-сервера**

Если ваш прокси-сервер требует аутентификации, в полях **Имя пользователя** и **Пароль** укажите учетные данные учетной записи, под которой устанавливается соединение с прокси-сервером. Рекомендуется указывать данные учетной записи с минимальными правами, необходимыми только для аутентификации на прокси-сервере.

5. При необходимости загрузите новый сертификат Сервера администрирования.

- **Смена виртуального Сервера на этом главном Сервере**

  Выберите этот параметр, чтобы переместить на виртуальный Сервер администрирования клиентские устройства на текущем главном Сервере администрирования. Для этого в раскрывающемся списке **Имя виртуального Сервера администрирования** выберите нужный виртуальный Сервер администрирования.

7. На шаге мастера **Выбор учетной записи для запуска задачи** укажите параметры учетной записи:

   - **Учетная запись по умолчанию**

     Задача будет запускаться под той же учетной записью, под которой было установлено и запущено приложение, выполняющее эту задачу.

     По умолчанию выбран этот вариант.

   - **Задать учетную запись**

     В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.

     - **Учетная запись**

       Учетная запись, от имени которой будет запускаться задача.

     - **Пароль**

       Пароль учетной записи, от имени которой будет запускаться задача.

8. Если требуется изменить параметры задачи по умолчанию, на шаге мастера **Завершение создания задачи** включите параметр **Открыть окно свойств задачи после ее создания**.

   Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

9. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.

10. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

11. Если вы хотите изменить параметры задачи по умолчанию, в окне свойств задачи укажите общие параметры задачи в соответствии с вашими требованиями.

12. Нажмите на кнопку **Сохранить**.

    Задача создана и настроена.

13. Запустите созданную задачу.

    После завершения работы задачи клиентские устройства, для которых она была создана, переходят под управление Сервера администрирования, указанного в параметрах задачи.

Удаление виртуального Сервера администрирования

При удалении виртуального Сервера администрирования все объекты, созданные на Сервере администрирования, включая политики и задачи, также будут удалены. Управляемые устройства из групп администрирования, которыми управлял виртуальный Сервер администрирования, будут удалены из групп администрирования. Чтобы вернуть устройства под управление Kaspersky Security Center, выполните опрос сети, а затем переместите найденные устройства из группы Нераспределенные устройства в группы администрирования.

Чтобы удалить виртуальный Сервер администрирования:

1. В главном меню нажмите на значок параметров ( ) рядом с именем Сервера администрирования.
2. На открывшейся странице выберите вкладку **Серверы администрирования**.
3. Выберите виртуальный Сервер администрирования, который вы хотите удалить.
4. В строке меню нажмите на кнопку **Удалить**.

   Виртуальный Сервер администрирования удален.

Включение защиты учетной записи от несанкционированного изменения

Вы можете дополнительно включить защиту учетной записи пользователя от несанкционированного изменения. Если этот параметр включен, изменение параметров учетной записи пользователя требует авторизации пользователя с правами на изменение.

Чтобы включить или выключить защиту учетной записи от несанкционированного изменения:

1. В главном окне приложения перейдите в раздел **Пользователи и роли → Пользователи**.
2. Нажмите на учетную запись внутреннего пользователя, для которой вы хотите настроить защиту учетной записи от несанкционированного изменения.
3. В открывшемся окне свойств пользователя выберите вкладку **Защита учетной записи**.

4. На вкладке **Защита учетной записи** выберите параметр **Запросить аутентификацию для проверки разрешения на изменение учетных записей пользователей**, если вы хотите запрашивать учетные данные каждый раз при изменении параметров учетной записи. В противном случае выберите **Разрешить пользователям изменять эту учетную запись без дополнительной аутентификации**.

5. Нажмите на кнопку **Сохранить**.

Для учетной записи пользователя включена защита от несанкционированного изменения.

Резервное копирование и восстановление данных Сервера администрирования

Резервное копирование данных позволяет переносить Сервер администрирования с одного устройства на другое без потерь информации. С помощью резервного копирования вы можете восстанавливать данные при переносе информационной базы Сервера администрирования на другое устройство или при переходе на более позднюю версию Kaspersky Security Center. Также вы можете использовать резервное копирование данных для переноса данных Сервера администрирования Kaspersky Security Center Windows под управление Kaspersky Security Center Linux (перенос данных из Kaspersky Security Center Linux в Kaspersky Security Center Windows не поддерживается).

Резервные копии установленных плагинов управления не сохраняются. После восстановления данных Сервера администрирования из резервной копии необходимо загрузить и переустановить плагины управляемых приложений.

Прежде чем создавать резервную копию данных Сервера администрирования, проверьте, добавлен ли виртуальный Сервер администрирования в группу администрирования. Если виртуальный Сервер администрирования добавляется перед резервным копированием, убедитесь, что этому виртуальному Серверу назначен администратор. Вы не можете предоставить права администратора к виртуальному Серверу администрирования после резервного копирования. Обратите внимание, если учетные данные администратора утеряны, вы не сможете назначить нового администратора виртуальному Серверу администратора.

Для резервного копирования или восстановления отказоустойчивого кластера Kaspersky Security Center нужно остановить весь кластер для обслуживания, а затем перезагрузить его после завершения резервного копирования или восстановления.

Вы можете создать резервную копию данных Сервера администрирования одним из следующих способов:

- Создать и запустить задачу резервного копирования данных через Консоль администрирования.
- Запустить утилиту klbackup на устройстве, где установлен Сервер администрирования. Утилита входит в состав комплекта поставки Kaspersky Security Center. После установки Сервера администрирования утилита находится в корне папки назначения, указанной при установке приложения.

В резервной копии данных Сервера администрирования сохраняются следующие данные:

- база данных Сервера администрирования (политики, задачи, параметры приложений, сохраненные на Сервере администрирования события);
- конфигурационная информация о структуре групп администрирования и клиентских устройствах;

- хранилище дистрибутивов приложений для удаленной установки;
- сертификат Сервера администрирования;
- Содержимое папки *Обновления*.

  По умолчанию путь к папке – C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\

Восстановление данных Сервера администрирования возможно только с помощью утилиты klbackup. Вам нужно выполнить восстановление на только что установленном и работоспособном экземпляре Сервера администрирования той версии, для которой была сделана резервная копия (или более новой).

Создание задачи резервного копирования данных

Задача резервного копирования является задачей Сервера администрирования и создается мастером первоначальной настройки. Если задача резервного копирования, созданная мастером первоначальной настройки, была удалена, вы можете создать ее вручную.

Чтобы создать задачу резервного копирования данных Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В окне мастера **Параметры новой задачи** выберите тип задачи **Резервное копирование данных Сервера администрирования**.
4. Следуйте дальнейшим шагам мастера.

Задачу **Резервное копирование данных Сервера администрирования** можно создать только в одном экземпляре. Если задача резервного копирования данных Сервера администрирования уже создана для Сервера администрирования, то она не отображается в окне выбора типа задачи мастера создания задачи резервного копирования.

Чтобы настроить задачу резервного копирования данных Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи** и выберите задачу **Резервное копирование данных Сервера администрирования**.
2. Нажмите на название задачи **Резервное копирование данных Сервера администрирования**.

   Откроется окно свойств задачи.
3. При необходимости укажите общие параметры задачи в соответствии с вашими требованиями.

4. В разделе **Параметры приложения** укажите путь к папке для хранения резервных копий данных Сервера администрирования, установите защиту паролем резервного копирования и количество резервных копий, если это необходимо.

5. Нажмите на кнопку **Сохранить**, чтобы применить изменения.

Задача *Резервное копирование данных Сервера администрирования* настроена.

Перенос Сервера администрирования на другое устройство

Если вам нужно использовать Сервер администрирования на новом устройстве, вы можете перенести его одним из следующих способов:

- Переместить Сервер администрирования и сервер базы данных на новое устройство (сервер базы данных может быть установлен на новом устройстве вместе с Сервером администрирования или на другом устройстве).
- Оставить сервер баз данных на старом устройстве и перенести на новое устройство только Сервер администрирования.

Чтобы перенести Сервер администрирования и сервер баз данных на новое устройство:

1. На предыдущем устройстве создайте резервную копию данных Сервера администрирования.

   Для этого запустите задачу резервного копирования данных с помощью Kaspersky Security Center Web Console или запустите утилиту klbackup.

   > Если вы используете SQL Server в качестве СУБД для Сервера администрирования, можно перенести данные с SQL Server на СУБД MySQL или MariaDB. Для создания резервной копии данных запустите утилиту klbackup в интерактивном режиме. В окне **Параметры резервного копирования** мастера резервного копирования и восстановления данных включите параметр **Перенос данных в формате MySQL/MariaDB**. Kaspersky Security Center создаст резервную копию, совместимую с MySQL и MariaDB. После этого вы можете восстановить данные из резервной копии в MySQL или MariaDB.

   > Также можно включить параметр **Перенести в формат Azure**, если вы хотите перенести данные из SQL Server в СУБД Azure SQL.

2. На предыдущем устройстве отключите Сервер администрирования от сети.

3. Выберите новое устройство, на которое будет установлен Сервер администрирования. Убедитесь, что аппаратное и программное обеспечение на выбранном устройстве соответствует требованиям для Сервера администрирования, Kaspersky Security Center Web Console и Агента администрирования. Проверьте, что порты, используемые на Сервере администрирования доступны.

4. Назначьте новому устройству тот же адрес.

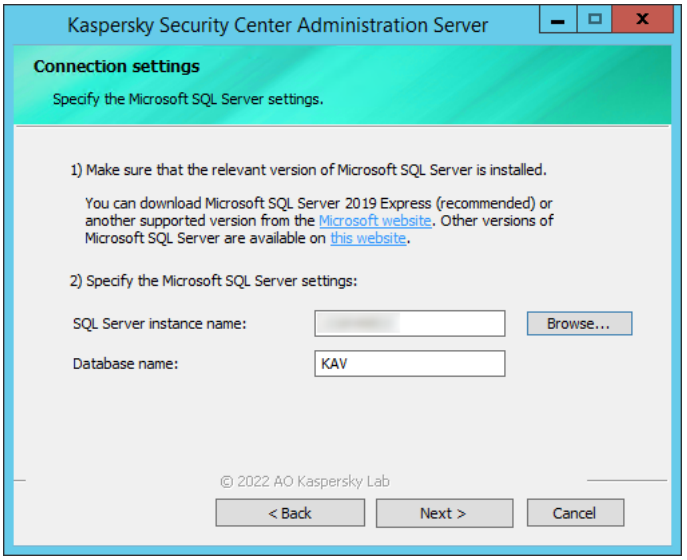
   Новому Серверу администрирования можно присвоить имя NetBIOS, FQDN и статический IP-адрес. Это зависит от того, какой адрес Сервера администрирования был установлен в инсталляционном пакете Агента администрирования, когда были развернуты Агенты администрирования. Также вы можете использовать адрес подключения, определяющий Сервер администрирования, к которому подключается Агент администрирования (вы можете получить этот адрес на управляемых устройствах с помощью утилиты klnagchk).

5. При необходимости на другом устройстве установите систему управления базами данных (СУБД), которую будет использовать Сервер администрирования.

   База данных может быть установлена на новом устройстве вместе с Сервером администрирования или на другом устройстве. Убедитесь, что это устройство соответствует аппаратным и программным требованиям. При выборе СУБД учитывайте количество устройств, которые обслуживает Сервер администрирования.

6. Запустите установку Сервера администрирования на новом устройстве.

7. Во время установки Сервера администрирования настройте параметры подключения к серверу баз данных.



Пример окна параметров подключения для Microsoft SQL Server

В зависимости от того, где вам нужно разместить сервер базы данных, выполните одно из следующих действий:

- **Оставьте сервер базы данных на предыдущем устройстве.**

  1. Нажмите на кнопку **Обзор** рядом с полем **Имя экземпляра SQL-сервера** и выберите имя предыдущего устройства в появившемся списке.

     Обратите внимание, что предыдущее устройство должно быть доступно для связи с новым Сервером администрирования.

  2. Введите имя предыдущей базы данных в поле **Имя базы данных**.

- **Переместите сервер базы данных на другое устройство.**

  1. Нажмите на кнопку **Обзор** рядом с полем **Имя экземпляра SQL-сервера** и выберите имя устройства в появившемся списке.

  2. Введите имя новой базы данных в поле **Имя базы данных**.

     Обратите внимание, что имя новой базы данных должно совпадать с именем базы данных на предыдущем устройстве. Имена баз должны совпадать, чтобы можно было использовать резервную копию Сервера администрирования. Имя базы данных по умолчанию *KAV*.

8. После завершения установки восстановите данные Сервера администрирования на новом устройстве с помощью утилиты klbackup.

   Если вы используете SQL Server в качестве СУБД на предыдущем и новом устройствах, обратите внимание, что версия SQL Server, установленная на новом устройстве, должна быть такой же или выше, чем версия SQL Server, установленная на предыдущем устройстве. Иначе вы не сможете восстановить данные Сервера администрирования на новом устройстве.

9. Откройте Kaspersky Security Center Web Console и подключитесь к Серверу администрирования.

10. Убедитесь, что все управляемые устройства подключены к Серверу администрирования.

11. Удалите Сервер администрирования и сервер баз данных с предыдущего устройства.

Также можно использовать Консоль администрирования, чтобы перенести Сервер администрирования и сервер базы данных на другое устройство.

Проверка целостности модулей с помощью утилит klscmodchk и integrity_checker

Kaspersky Security Center содержит двоичные модули в виде динамически подключаемых библиотек, исполняемых файлов, конфигурационных файлов и файлов интерфейса. Злоумышленники могут заменить один или несколько исполняемых модулей или файлов приложений другими файлами, содержащими вредоносный код. Для предотвращения подмены модулей и файлов в Kaspersky Security Center реализована проверка целостности компонентов с помощью утилит klscmodchk и integrity_checker. Эти утилиты проверяют модули и файлы на предмет несанкционированных изменений или повреждений. Если модуль или файл приложения имеют неверную контрольную сумму, они считаются поврежденными.

Утилита klscmodchk выполняет проверку целостности следующих компонентов Kaspersky Security Center:

- Сервер администрирования
- Агент администрирования

Утилита integrity_checker выполняет проверку целостности следующих компонентов Kaspersky Security Center:

- Сервер администрирования
- Агент администрирования
- Kaspersky Security Center Web Console

Обе утилиты проверяют целостность модуля на основе файла манифеста kl_file_integrity_manifest.xml, который входит в сборку Kaspersky Security Center и находится в папке установки. Файл манифеста компонента содержит файлы, целостность которых важна для корректной работы компонента Kaspersky Security Center. Также проверяется целостность самих файлов манифеста.

Настоятельно не рекомендуется изменять файл манифеста kl_file_integrity_manifest.xml, так как цифровая подпись будет недействительна и это приведет к сбою проверки целостности.

Чтобы проверить целостность компонента Kaspersky Security Center, выполните одну из следующих команд:

- `$ klscmodchk [ параметры ]`

  Утилита klscmodchk запускает утилиту integrity_checker с параметром `--verbose` и проверяет целостность модулей.

  Параметры утилиты klscmodchk:

  - `-logfile <log_file_path>` – задает путь к файлу на диске для ведения журнала. По умолчанию информация выводится на консоли.
  - `-verbose` – отображает расширенную информацию во время проверки целостности.

- `$ integrity_checker [ параметры ] <путь_к_файлу_манифеста>`

  Параметры утилиты integrity_checker:

  - `--help` – отображает справку утилиты integrity_checker.
  - `--version` – отображает версию утилиты integrity_checker.
  - `--verbose` – отображает информацию о работе утилиты. При выполнении проверки целостности достаточно использовать этот параметр в команде.

Результат проверки каждого файла манифеста отображается рядом с именем файла манифеста в следующем формате:

- SUCCEEDED – целостность файла подтверждена (код возврата 0).
- FAILED – целостность файла не подтверждена (ненулевой код возврата).

Вы также можете настроить автоматический запуск проверки целостности при запуске приложения. По умолчанию автоматическая проверка целостности выключена.

Чтобы включить автоматическую проверку целостности:

1. На устройстве, на котором установлен Сервер администрирования, в командной строке Windows выполните следующую команду:

   ```
   klscflag.exe -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. Перезагрузите службу Сервера администрирования.

Автоматическая проверка целостности будет включена.

При следующем запуске Kaspersky Security Center утилита klscmodchk запустится вместе с Сервером администрирования и запустит проверку целостности модулей. Результат проверки целостности записывается в журнал Kaspersky Event Log.

Первоначальная настройка Kaspersky Security Center Web Console

В этом разделе описаны шаги, которые необходимо выполнить после установки Kaspersky Security Center Web Console для первоначальной настройки.

Мастер первоначальной настройки (Kaspersky Security Center Web Console)

В этом разделе представлена информация о работе мастера первоначальной настройки Сервера администрирования.

Мастеру требуется доступ в интернет. Если Сервер администрирования не имеет доступа в интернет, рекомендуется выполнять все шаги мастера вручную через интерфейс Kaspersky Security Center Web Console.

Приложение Kaspersky Security Center позволяет настроить минимальный набор параметров, необходимых для построения централизованной системы управления, обеспечивающей защиту сети от угроз безопасности. Эта настройка выполняется в мастере первоначальной настройки. В процессе работы мастера вы можете внести в приложение следующие изменения:

- Добавить файлы ключей или ввести коды активации, которые можно автоматически распространять на устройства в группах администрирования.
- Настроить взаимодействие с Kaspersky Security Network (KSN). При разрешении использования KSN мастер включает службу прокси-сервера KSN, которая обеспечивает взаимодействие между KSN и устройствами.
- Настроить рассылку по электронной почте оповещений о событиях в работе Сервера администрирования и управляемых приложений (чтобы уведомление прошло успешно, на Сервере администрирования и на всех устройствах-получателях должна быть запущена служба сообщений Messenger).
- Сформировать политику защиты рабочих станций и серверов, а также задачи поиска вредоносного ПО, получения обновлений и резервного копирования данных для верхнего уровня иерархии управляемых устройств.

  Мастер первоначальной настройки создает политики только для приложений, для которых еще нет созданных политик в папке **Управляемые устройства**. Мастер первоначальной настройки не создает задачи, если задачи с такими именами уже созданы для верхнего уровня иерархии управляемых устройств.

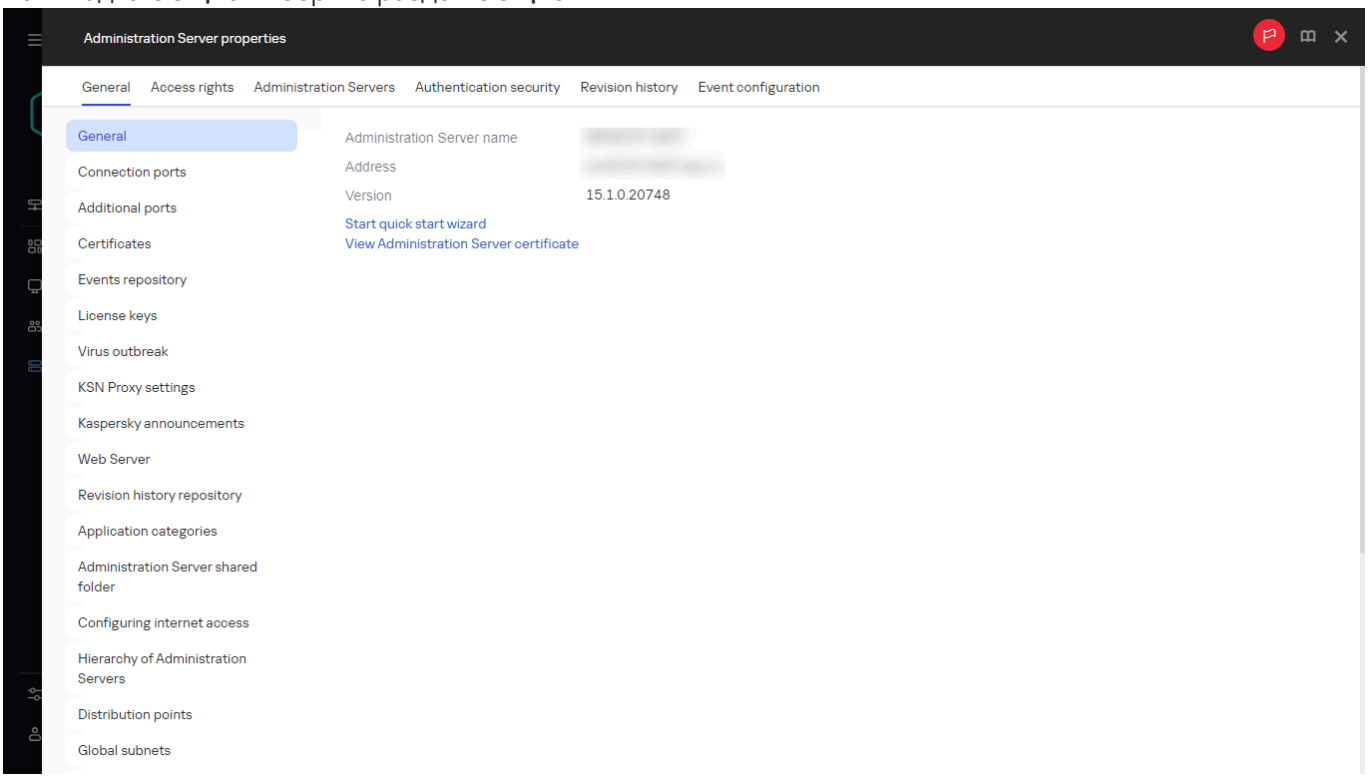
Приложение автоматически предлагает запустить мастер первоначальной настройки после установки Сервера администрирования при первом подключении к Серверу. Вы также можете запустить мастер первоначальной настройки вручную в любое время.

Чтобы запустить мастер первоначальной настройки вручную:

1. В главном меню нажмите на значок параметров ( ) рядом с именем Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Общие**.



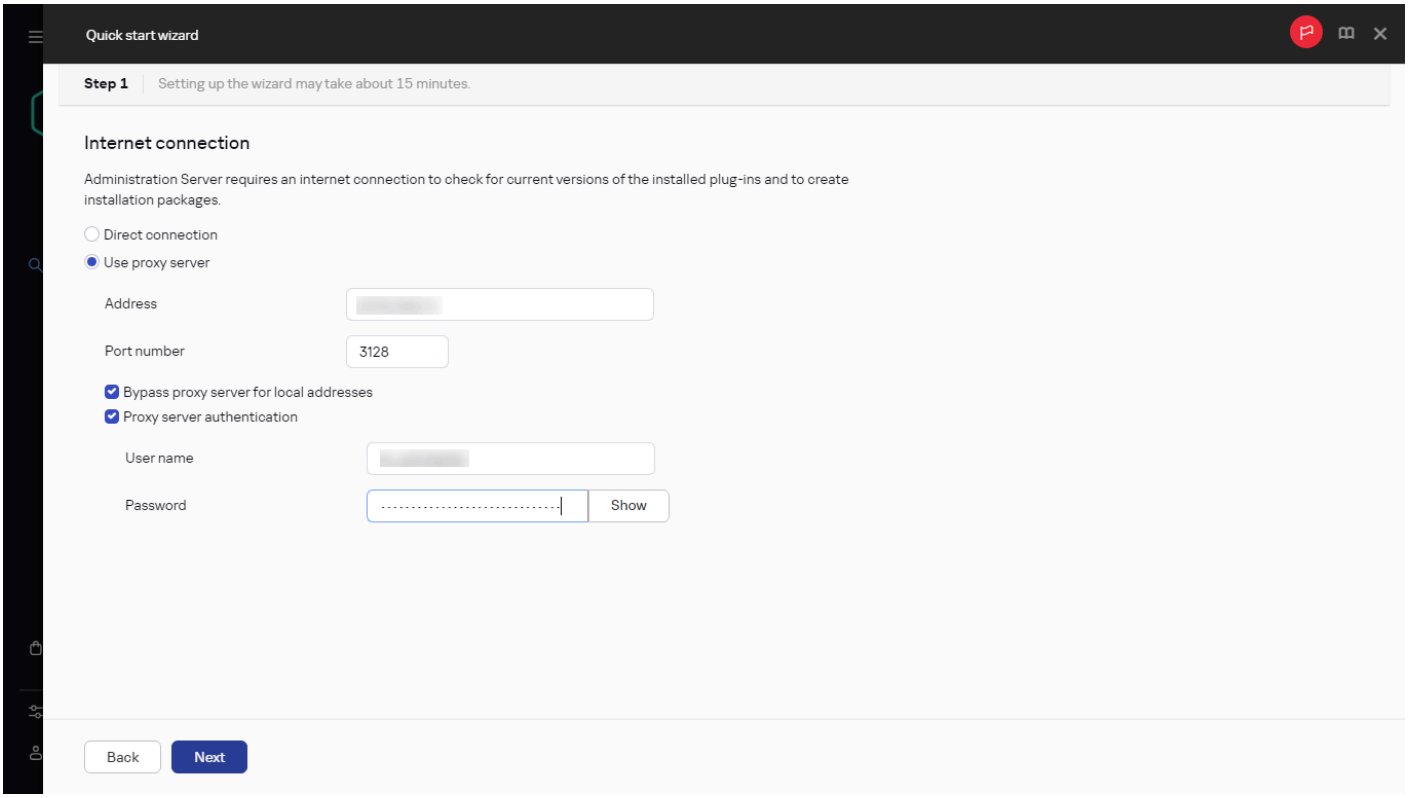
Окно свойств Сервера администрирования

3. Нажмите на кнопку **Запустить мастер первоначальной настройки**.

Мастер предложит произвести первоначальную настройку Сервера администрирования. Следуйте далее указаниям мастера. Для продолжения работы мастера нажмите на кнопку **Далее**.

Шаг 1. Указание параметров подключения к интернету

Укажите параметры доступа Сервера администрирования к интернету. Доступ к интернету необходимо настроить, чтобы использовать Kaspersky Security Network и загружать обновления антивирусных баз для Kaspersky Security Center и управляемых приложений "Лаборатории Касперского".



Параметры подключения к интернету

Включите параметр **Использовать прокси-сервер**, если требуется использовать прокси-сервер для подключения к интернету. Если параметр включен, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

- **Адрес**

  Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.

- **Номер порта**

  Номер порта, через который будет установлено прокси-подключение Kaspersky Security Center.

- **Не использовать прокси-сервер для локальных адресов**

  При подключении к устройствам в локальной сети не будет использоваться прокси-сервер.

- **Аутентификация на прокси-сервере**

  Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  Поле ввода доступно, если установлен флажок **Использовать прокси-сервер**.

- **Имя пользователя**

  Учетная запись пользователя, от имени которого будет выполняться подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

- **Пароль**

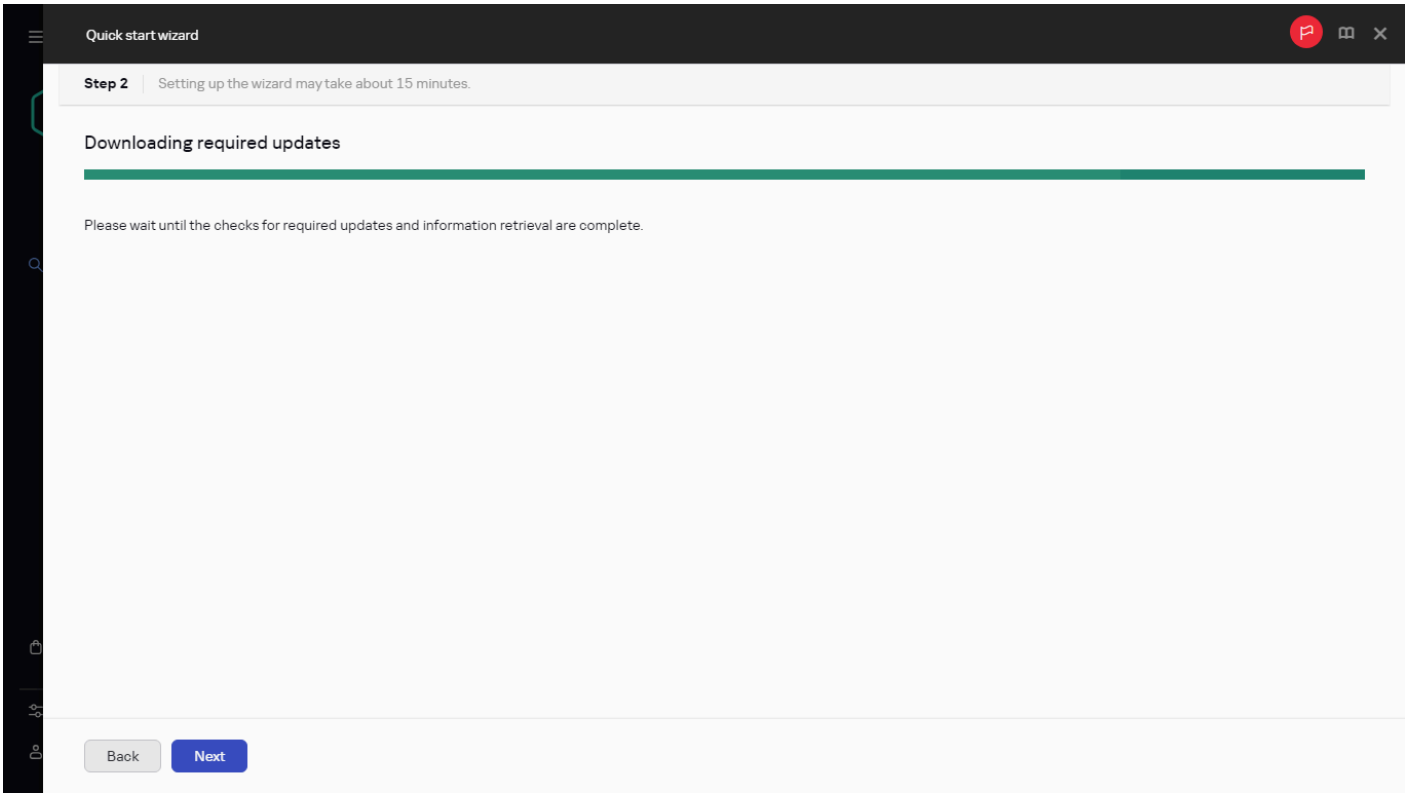
  Пароль пользователя, с помощью учетной записи которого выполняется подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

  Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

Вы можете настроить доступ в интернет позднее без запуска мастера первоначальной настройки.

Шаг 2. Загрузка требуемых обновлений

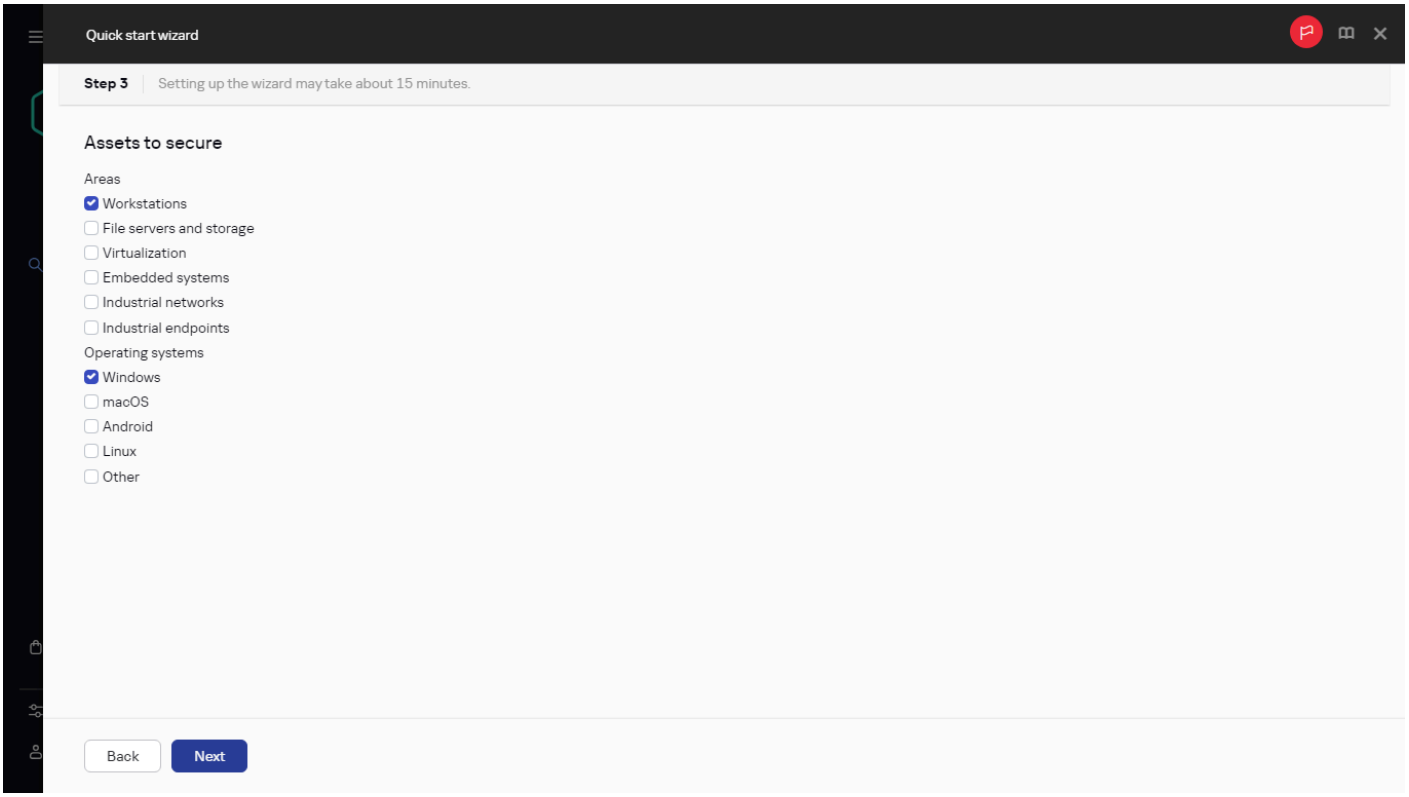
Необходимые обновления загружаются с серверов "Лаборатории Касперского" автоматически.



Загрузка требуемых обновлений

Шаг 3. Выбор активов для защиты

Выберите области защиты и операционные системы, которые используются в вашей сети. При выборе этих параметров вы указываете фильтры для плагинов управления приложениями и дистрибутивов на серверах "Лаборатории Касперского", которые вы можете загрузить для установки на клиентские устройства в вашей сети.



Выбор активов для защиты

Выберите следующие параметры:

- **Области**

  Вы можете выбрать одну из следующих областей защиты:

  - **Рабочие станции**. Выберите этот параметр, если вы хотите защитить рабочие станции в вашей сети. По умолчанию выбран параметр Рабочая станция.

  - **Файловые серверы и системы хранения данных**. Выберите этот параметр, если вы хотите защитить файловые серверы в вашей сети.

  - **Мобильные устройства**. Выберите этот параметр, если вы хотите защитить мобильные устройства, принадлежащие организации или сотрудникам организации. Если вы выбрали этот параметр, но не предоставили лицензию с возможностью Управление мобильными устройствами, отобразится сообщение о необходимости предоставить лицензию с возможностью Управление мобильными устройствами. Без этой лицензии использование возможностей Управления мобильными устройствами невозможно.

  - **Виртуальные среды**. Выберите этот параметр, если вы хотите защитить виртуальные машины в вашей сети.

  - **Анти-Спам**. Выберите этот параметр, если вы хотите защитить почтовые серверы вашей организации от спама, мошенничества и доставки вредоносных приложений.

  - **Банкоматы и POS-системы**. Выберите этот параметр, если вы хотите защитить встроенные системы с операционной системой Windows, например банкоматы (ATM).

- **Промышленные сети**. Выберите этот параметр, если вы хотите контролировать данные безопасности в промышленной сети и с конечных устройств сети, защищенных приложениями "Лаборатории Касперского".

- **Промышленные конечные точки**. Выберите этот параметр, если вы хотите защитить отдельные узлы промышленной сети.

- **Операционные системы**

  Вы можете выбрать одну из следующих платформ:

  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - Другое

  Дополнительные сведения о поддерживаемых версиях операционных систем см. в разделе Аппаратные и программные требования Kaspersky Security Center Web Console.

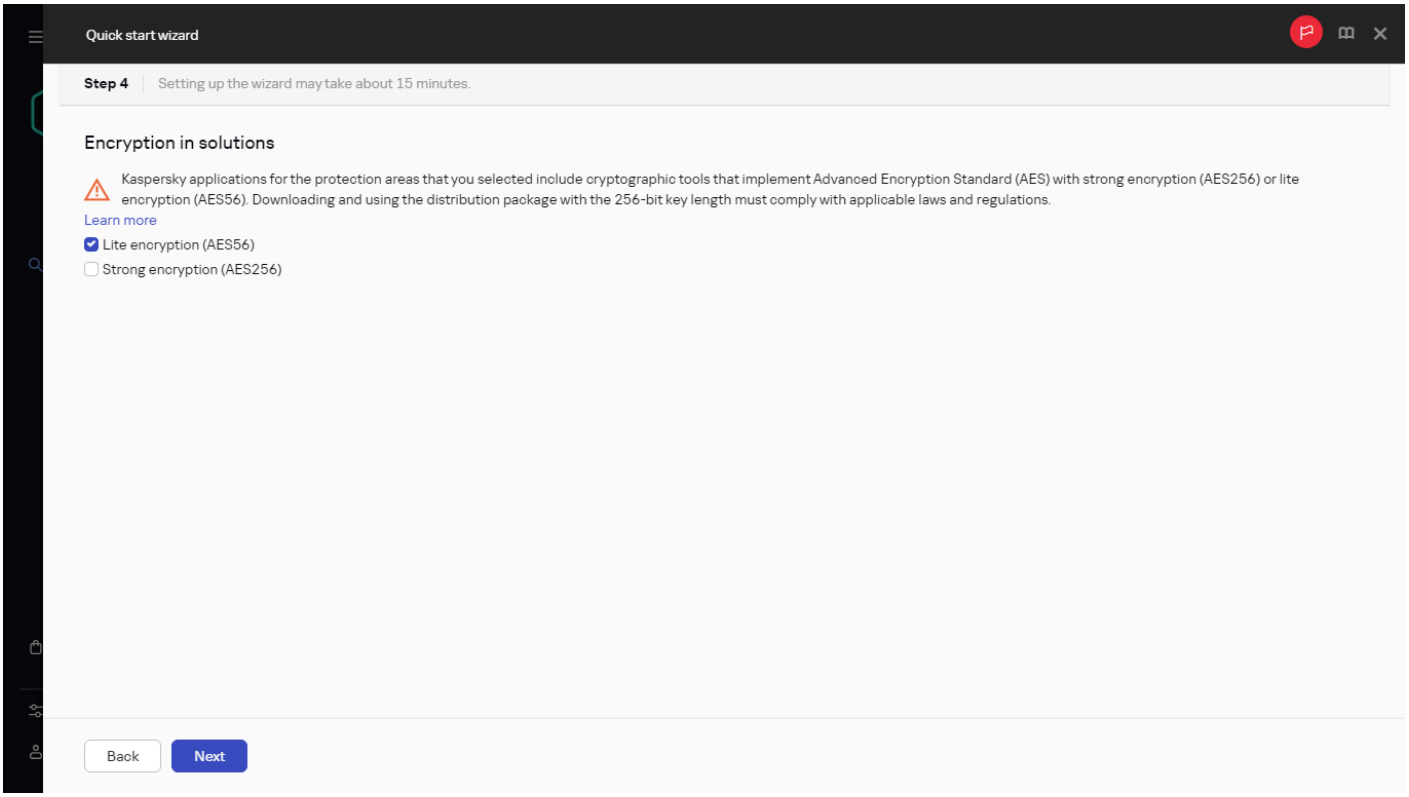
Можно выбрать инсталляционные пакеты приложений "Лаборатории Касперского" из списка доступных инсталляционных пакетов позднее без запуска мастера первоначальной настройки. Для упрощения поиска необходимых инсталляционных пакетов вы можете фильтровать список доступных инсталляционных пакетов различным критериям.

Шаг 4. Выбор шифрования

Окно **Шифрование** отображается, только если в качестве области защиты выбран вариант **Рабочие станции**.

Kaspersky Endpoint Security для Windows включает инструменты шифрования информации, хранящейся на клиентских устройствах в операционной системой Windows. Эти инструменты шифрования имеют расширенный стандарт шифрования (AES), реализованный с длиной ключа 256 бит или 56 бит.

Загрузка и использование дистрибутива с длиной ключа 256 бит должна выполняться в соответствии с действующими законами и правилами. Чтобы загрузить дистрибутив Kaspersky Endpoint Security для Windows, действительный для нужд вашей организации, обратитесь к законодательству страны, в которой расположены клиентские устройства вашей организации.



Выбор шифрования

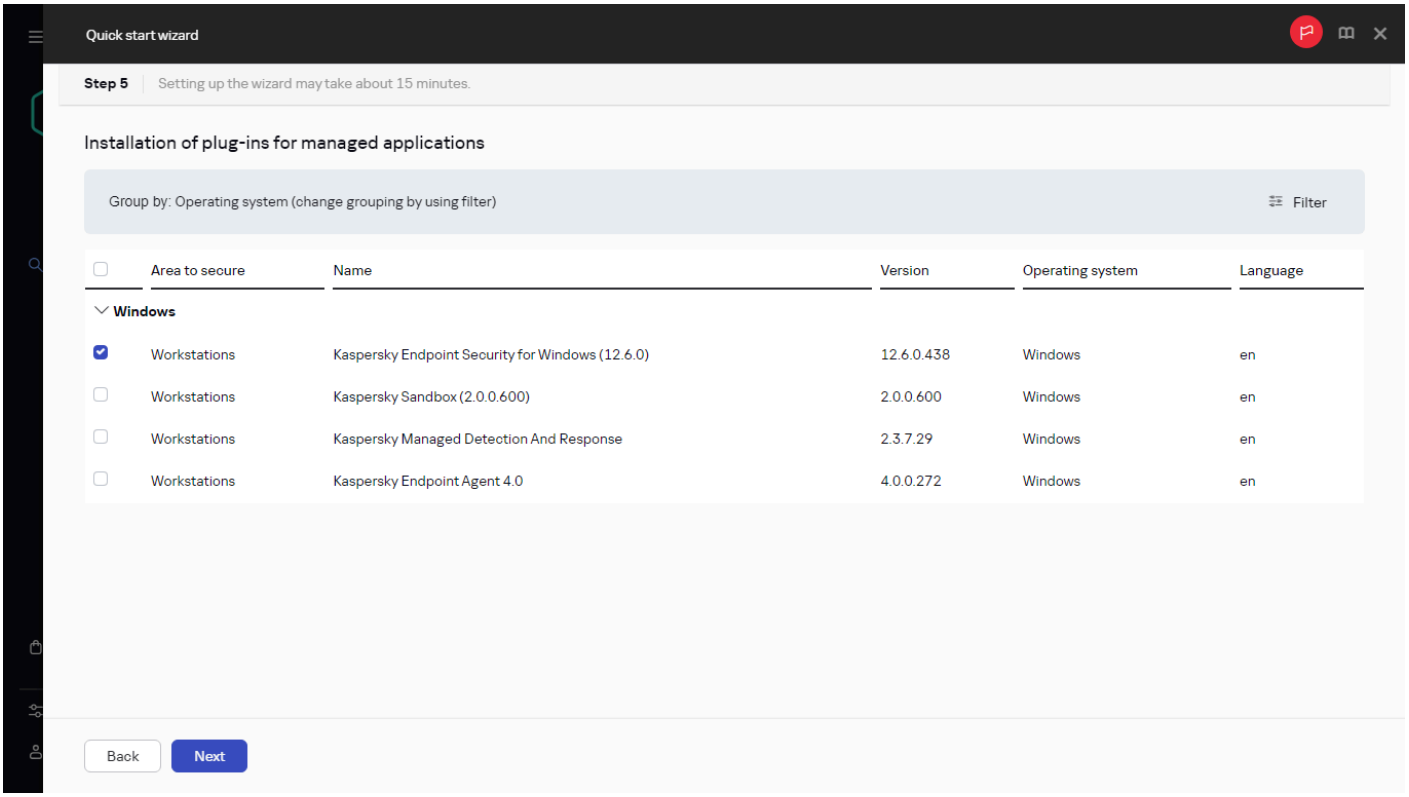
В окне **Шифрование** выберите один из следующих типов шифрования:

- Быстрое шифрование. Для этого типа шифрования используется 56-разрядный ключ.
- Стойкое шифрование. Для этого типа шифрования используется 256-разрядный ключ.

Вы можете выбрать дистрибутив для Kaspersky Endpoint Security для Windows с необходимым типом шифрования позднее без запуска мастера первоначальной настройки.

Шаг 5. Настройка установки плагинов для управляемых приложений

Выберите плагины для управляемых приложений для установки. Отображается список плагинов, расположенных на серверах "Лаборатории Касперского". Список отфильтрован в соответствии с параметрами, выбранными на предыдущем шаге мастера. По умолчанию в полный список включены плагины всех языков. Чтобы отображался только плагин на выбранном языке, используйте фильтр.



Установка плагинов для управляемых приложений

Список плагинов включает в себя следующие столбцы:

- **Область защиты**

  В этом столбце отображаются выбранные области для защиты.

- **Тип**

  В этом столбце отображаются типы плагинов.

- **Имя**

  Выбраны плагины в зависимости от областей защиты и платформ, выбранных на предыдущем шаге.

- **Версия**

  В список включены плагины всех версий, размещенных на серверах "Лаборатории Касперского". По умолчанию выбраны плагины последних версий.

- **Последняя версия**

  В этом столбце указано, является ли версия плагина последней. Если отображается значение **true**, соответствующий плагин имеет последнюю версию. Если отображается значение **false**, для соответствующего плагина существует более поздняя версия.

- **Операционная система**

  В этом столбце отображаются плагины операционных систем.

- **Язык**

  По умолчанию язык локализации плагина зависит от языка Kaspersky Security Center, который вы выбрали при установке. Другие языки можно выбрать в раскрывающемся списке **Отображать язык Консоли администрирования или**.

После выбора плагинов нажмите на кнопку **Далее**, чтобы начать установку.

Вы можете установить плагины управления для приложений "Лаборатории Касперского" вручную позднее без запуска мастера первоначальной настройки.

Мастер первоначальной настройки автоматически установит выбранные плагины. Для установки некоторых плагинов вам нужно принять условия Лицензионного соглашения. Ознакомьтесь с текстом Лицензионного соглашения, который отображается на экране, установите флажок **Я принимаю условия использования Kaspersky Security Network** и нажмите на кнопку **Установить**. Если вы не согласны с условиями Лицензионного соглашения, плагин не установится.

Когда все выбранные плагины будут установлены, мастер первоначальной настройки автоматически перейдет к следующему шагу.

Шаг 6. Установка выбранных плагинов

Мастер первоначальной настройки автоматически устанавливает плагины, выбранные на предыдущем шаге. Для установки некоторых плагинов вам нужно принять условия Лицензионного соглашения. Ознакомьтесь с текстом Лицензионного соглашения, который отображается на экране, установите флажок **Я принимаю условия использования Kaspersky Security Network** и нажмите на кнопку **Установить**. Если вы не согласны с условиями Лицензионного соглашения, плагин не установится.

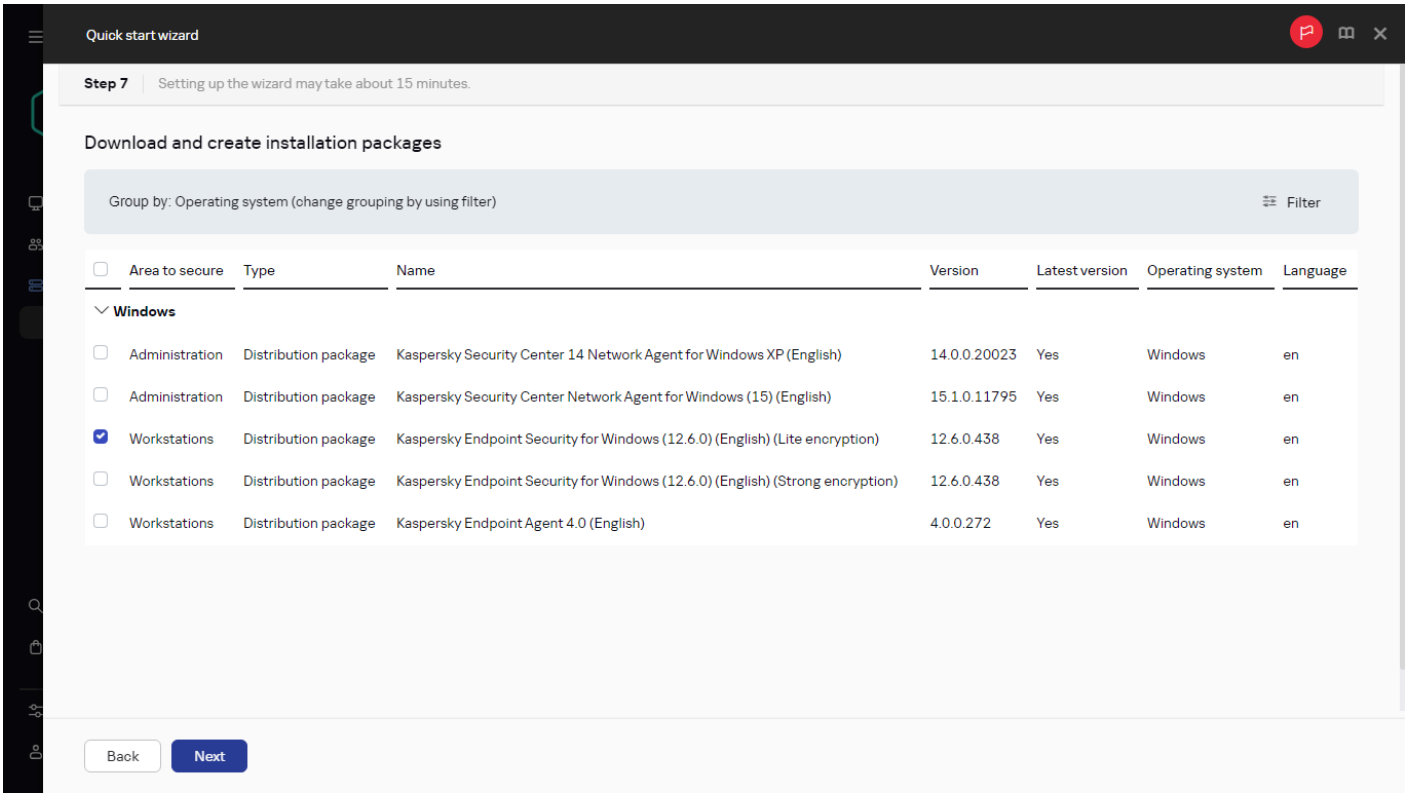
Когда все выбранные плагины будут установлены, мастер первоначальной настройки автоматически перейдет к следующему шагу.

Шаг 7. Загрузка дистрибутивов и создание инсталляционных пакетов

Выберите дистрибутив для загрузки.

Для дистрибутивов управляемых приложений может потребоваться установка определенной минимальной версии Kaspersky Security Center.

После того, как вы выбрали тип шифрования для Kaspersky Endpoint Security для Windows, отобразится список дистрибутивов для обоих типов шифрования. В списке выбран дистрибутив с выбранным типом шифрования. Вы можете выбрать дистрибутив для любого типа шифрования. Язык дистрибутива соответствует языку Kaspersky Security Center. Если дистрибутив Kaspersky Endpoint Security для Windows для языка Kaspersky Security Center не существует, выбирается дистрибутив на английском языке.



Загрузка дистрибутивов и создание инсталляционных пакетов

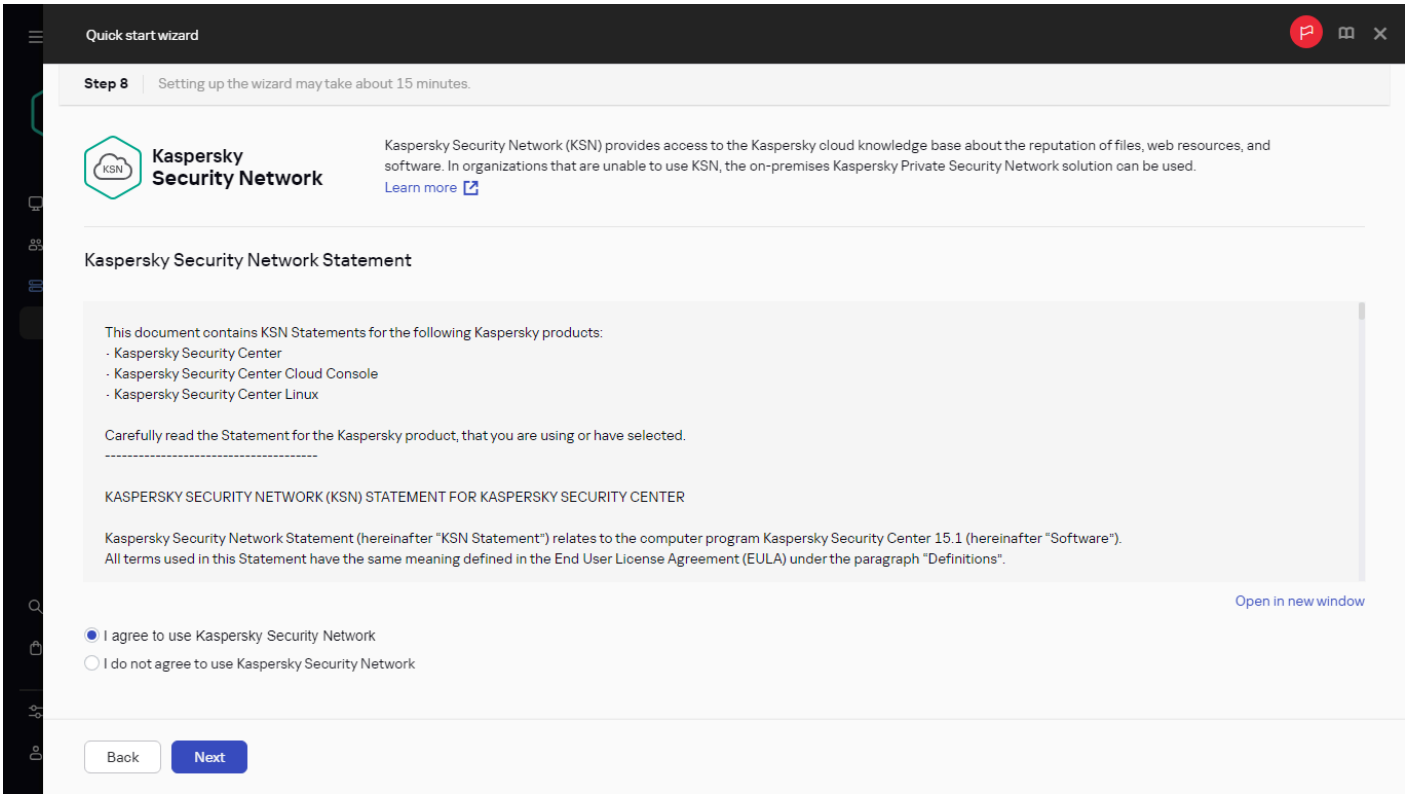
Чтобы завершить загрузку некоторых дистрибутивов вам нужно принять Лицензионное соглашение. При нажатии кнопки **Принять** отображается текст Лицензионного соглашения. Чтобы перейти к следующему шагу мастера, вам нужно принять положения и условия Лицензионного соглашения, а также условия Политики конфиденциальности "Лаборатории Касперского". Если вы не принимаете положения и условия, загрузка пакета отменяется.

После того, как вы приняли положения и условия Лицензионного соглашения, а также условия Политики конфиденциальности "Лаборатории Касперского", загрузка дистрибутивов продолжается. В дальнейшем инсталляционные пакеты можно использовать для развертывания приложений "Лаборатории Касперского" на клиентских устройствах.

Вы можете загрузить дистрибутивы и создать инсталляционные пакеты позднее без запуска мастера первоначальной настройки.

Шаг 8. Настройка Kaspersky Security Network

Настройте параметры передачи информации о работе Kaspersky Security Center в базу знаний Kaspersky Security Network.



Настройка Kaspersky Security Network

Выберите один из следующих вариантов:

- **Я принимаю условия использования Kaspersky Security Network**

  Kaspersky Security Center 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 и управляемые приложения не будут предоставлять информацию о своей работе Kaspersky Security Network.

  Если вы выбрали этот параметр, использование Kaspersky Security Network будет выключено.

Вы можете настроить доступ к Kaspersky Security Network (KSN) позднее без запуска мастера первоначальной настройки.

Шаг 9. Выбор способа активации приложения

Выберите один из следующих вариантов активации Kaspersky Security Center:

- **Введите ваш код активации**

  Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить ключ, активирующий Kaspersky Security Center. Код активации отправляется вам на адрес электронной почты, указанный при приобретении Kaspersky Security Center.

Чтобы активировать приложение с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Если вы выбрали этот вариант активации приложения, можно включить параметр **Автоматически распространять лицензионный ключ на управляемые устройства**.

Если выбран этот вариант, лицензионный ключ будет распространяться на управляемые устройства автоматически.

Если этот вариант не выбран, лицензионный ключ можно будет распространить на управляемые устройства позже, в папке **Лицензии "Лаборатории Касперского"** дерева консоли администрирования.

- **Укажите файл ключа**

  Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления ключа, активирующего приложение.

  Способы получения файла ключа описаны в разделе О файле ключа.

  Чтобы активировать приложение с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

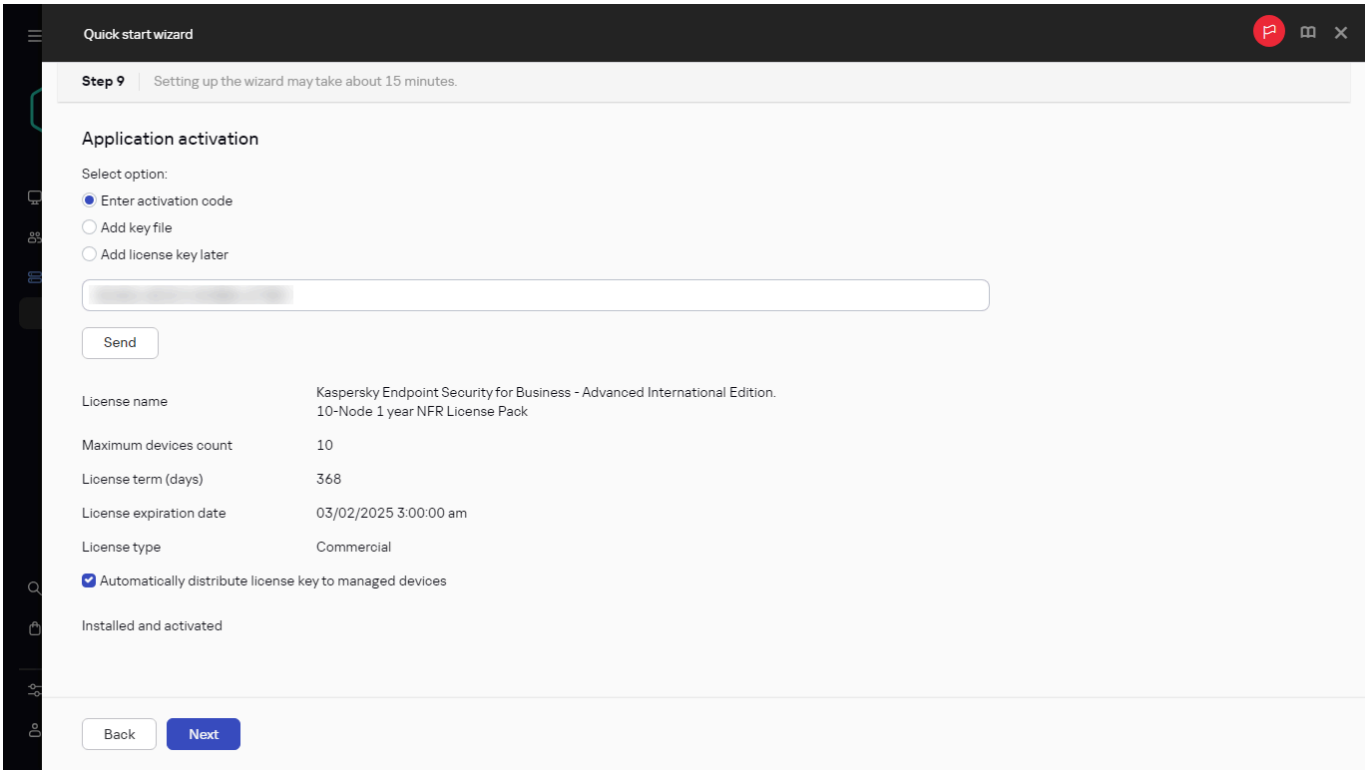
  Если вы выбрали этот вариант активации приложения, можно включить параметр **Автоматически распространять лицензионный ключ на управляемые устройства**.

  Если выбран этот вариант, лицензионный ключ будет распространяться на управляемые устройства автоматически.

  Если этот вариант не выбран, лицензионный ключ можно будет распространить на управляемые устройства позже, в папке **Лицензии "Лаборатории Касперского"** дерева консоли администрирования.

- **Отложите активацию приложения**

  Приложение будет работать в режиме Базовой функциональности, без поддержки Управления мобильными устройствами и Системного администрирования.



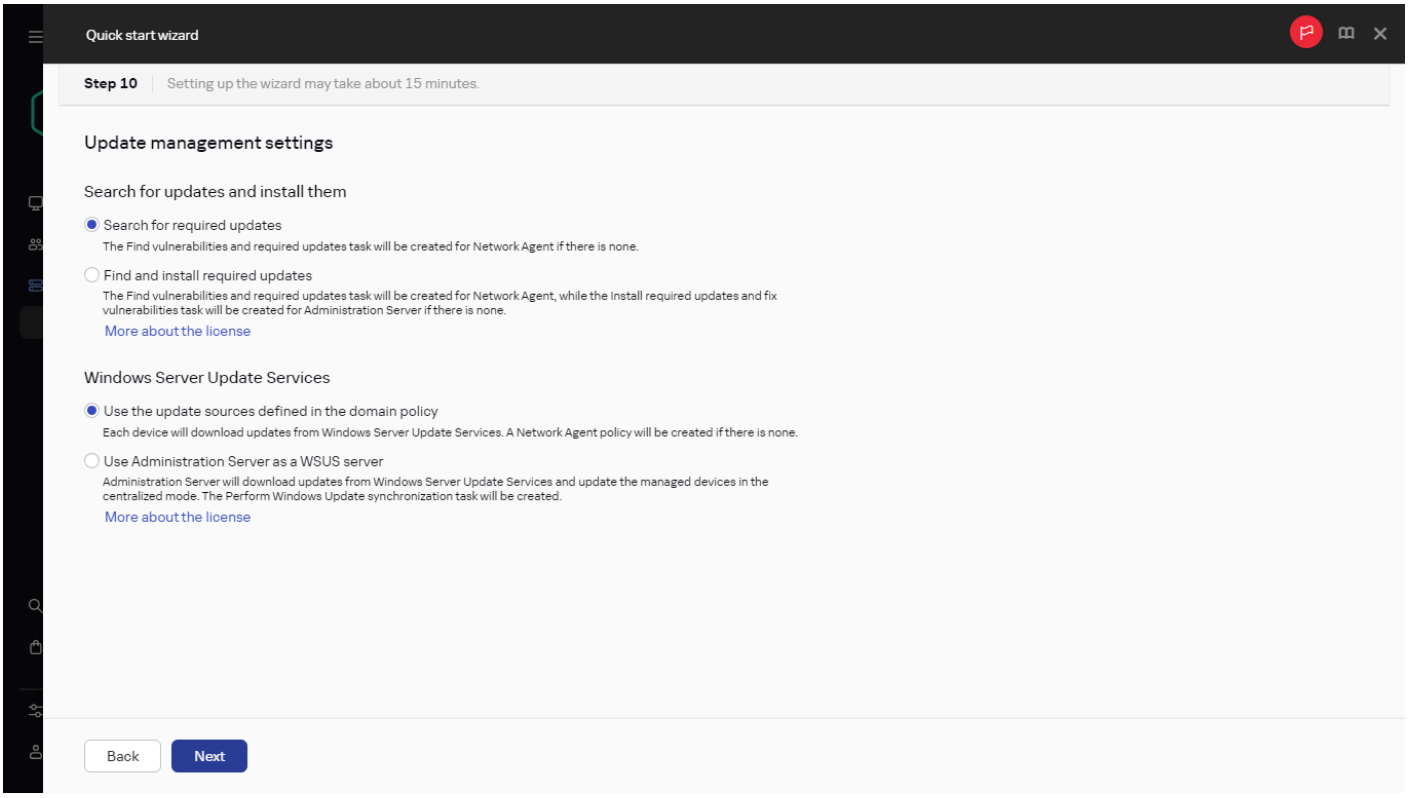
Выбор способа активации приложения

Если вы отложили активацию приложения, вы можете добавить ключ позже в любое время, выбрав **Операции → Лицензирование**.

При работе с Kaspersky Security Center, развернутым из платного образа AMI или с использованием ежемесячных счетов за использование SKU, вы не можете указать файл ключа или ввести код активации.

Шаг 10. Указание параметров управления обновлениями приложений сторонних производителей

Этот шаг не отображается, если у вас нет лицензии на Системное администрирование, а задача *Поиск уязвимостей и требуемых обновлений* уже существует.



Управление параметрами обновлений приложений сторонних приложений

Для обновлений приложений сторонних производителей выберите один из следующих вариантов:

- **Искать требуемые обновления**

  Задача *Поиск уязвимостей и требуемых обновлений* создается автоматически, если она еще не создана.

  По умолчанию этот вариант выбран.

- **Искать и устанавливать требующиеся обновления**

  Задачи *Поиск уязвимостей и требуемых обновлений* и *Установка требуемых обновлений и закрытие уязвимостей* создаются автоматически, если они не были созданы ранее.

  Этот параметр доступен при наличии лицензии на Системное администрирование.

Для обновлений Центра обновления Windows выберите один из следующих вариантов:

- **Использовать источники обновлений, определенные в политике домена**

  Обновления Центра обновления Windows загружаются на клиентские устройства в соответствии с параметрами политики домена. Политика Агента администрирования создается автоматически, если она не была создана ранее.

- **Использовать Сервер администрирования в роли WSUS-сервера**

  Обновления Центра обновления Windows загружаются на клиентские устройства с Сервера администрирования. Задача *Синхронизация обновлений Windows Update* и политика Агента администрирования создаются автоматически, если они не были созданы ранее.

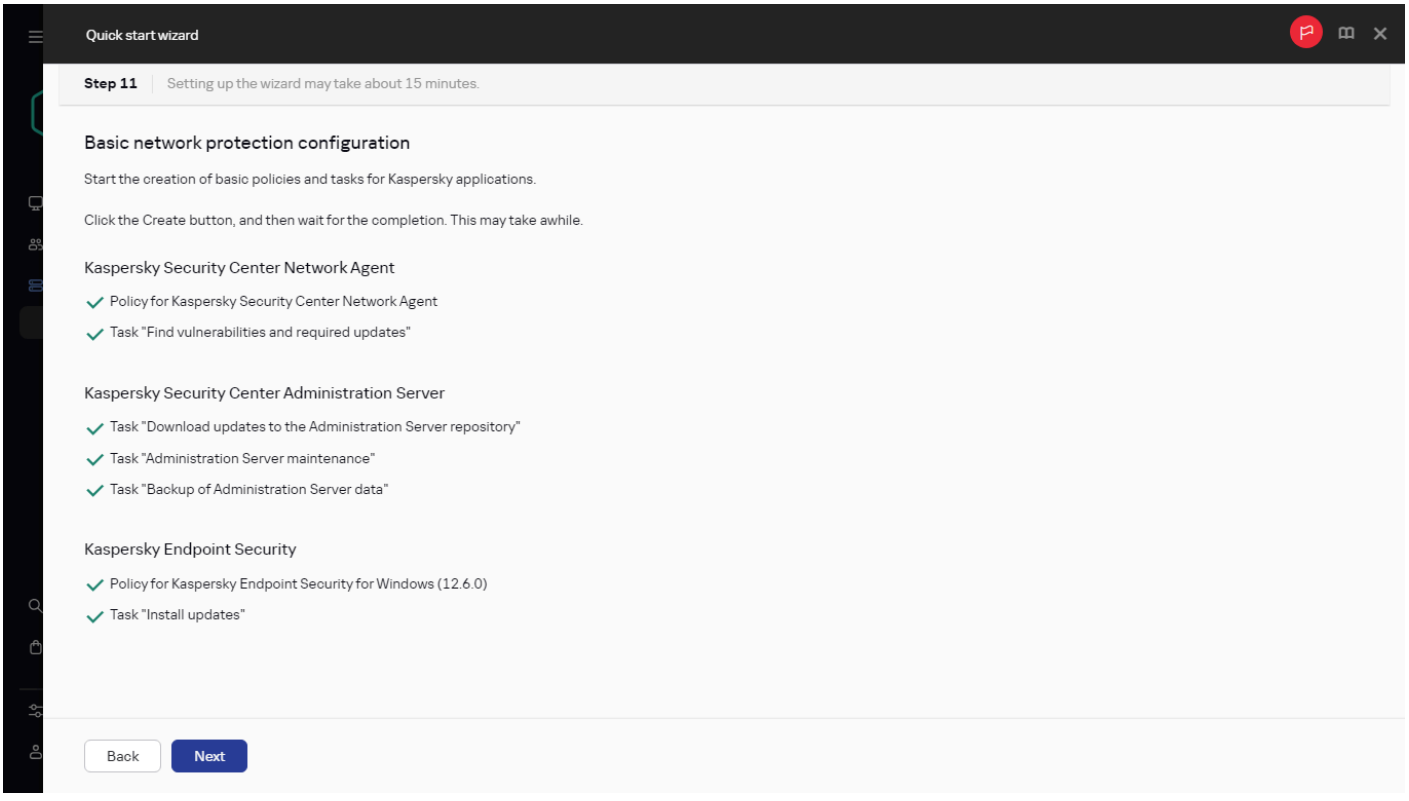
  Этот параметр доступен при наличии лицензии на Системное администрирование.

Вы можете создать задачи *Поиск уязвимостей и требуемых обновлений* и *Установка требуемых обновлений и закрытие уязвимостей* позднее без запуска мастера первоначальной настройки. Чтобы использовать Сервер администрирования в качестве WSUS-сервера, вам нужно создать задачу *Синхронизация обновлений Windows Update* и выбрать параметр **Использовать Сервер администрирования в роли WSUS-сервера** в политике Агента администрирования.

Шаг 11. Создание базовой конфигурации защиты сети

Вы можете проверить список созданных политик и задач.

Для перехода на следующий шаг мастера дождитесь окончания создания политик и задач.

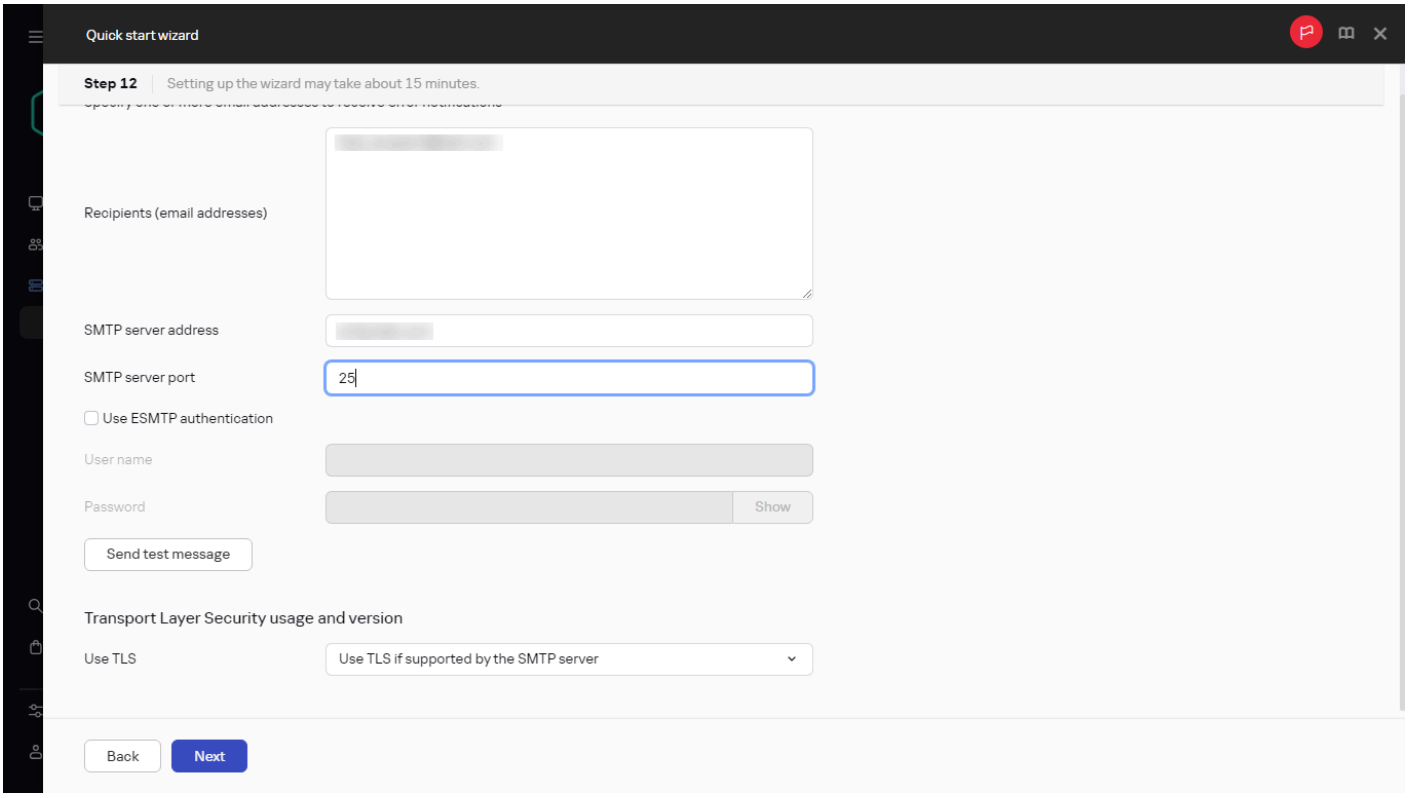


Создание базовой конфигурации защиты сети

Можно создать необходимые задачи и политики позднее без запуска мастера первоначальной настройки.

Шаг 12. Настройка параметров отправки уведомлений по электронной почте

Настройте параметры рассылки оповещений о событиях, регистрируемых при работе приложений "Лаборатории Касперского" на клиентских устройствах. Эти параметры будут использоваться в качестве значений по умолчанию в политиках приложений.



Настройка параметров отправки уведомлений по электронной почте

Для настройки рассылки оповещений о возникающих событиях приложений "Лаборатории Касперского" доступны следующие параметры:

- **Получатели (адреса электронной почты)**

  Адреса электронной почты пользователей, которым приложение будет отправлять уведомления. Вы можете указать один или более адресов. Если вы указываете несколько адресов, разделяйте их точкой с запятой.

- **Адрес SMTP-сервера**

  Адрес или адреса почтовых серверов вашей организации.

  Если вы указываете несколько адресов, разделяйте их точкой с запятой. Вы можете использовать следующие значения параметра:

  - IPv4-адрес или IPv6-адрес;
  - Имя устройства в сети Windows (NetBIOS-имя);
  - DNS-имя SMTP-сервера.

- **Порт SMTP-сервера**

  Номер коммуникационного порта SMTP-сервера. Если вы используете несколько SMTP-серверов, соединение с ними устанавливается через указанный коммуникационный порт. По умолчанию установлен порт 25.

- **Использовать ESMTP-аутентификацию**

  Включение поддержки ESMTP-аутентификации. После установки флажка можно указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию флажок снят.

- **Использовать TLS**

  Вы можете указать параметры подключения TLS для SMTP-сервера:

  - **Не использовать TLS**

    Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

  - **Использовать TLS, если поддерживается SMTP-сервером**

    Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.

  - **Всегда использовать TLS, для проверки срока действия сертификата сервера**

    Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

    > Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

    Если вы выбрали значение **Всегда использовать TLS, для проверки срока действия сертификата сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

  Вы можете указать сертификат для TLS подключения, перейдя по ссылке **Задать сертификаты**:

  - Выберите файл сертификата SMTP-сервера:

    Вы можете получить файл со списком сертификатов от доверенного центра сертификации и загрузить его на Сервер администрирования. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также доверенным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от доверенного центра сертификации.

  - Выберите файл сертификата клиента:

Вы можете использовать сертификат, полученный из любого источника, например, от любого доверенного центра сертификации. Вам нужно указать сертификат и его закрытый ключ, используя один из следующих типов сертификатов:

- Сертификат X-509:

  Вам нужно указать файл с сертификатом и файл с закрытым ключом. Оба файла не зависят друг от друга. Порядок загрузки файлов не имеет значения. Когда оба файла загружены, необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

- Контейнер pkcs12:

  Вам нужно загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

Вы можете проверить параметры уведомления о сообщениях электронной почты с помощью кнопки **Отправить тестовое сообщение**.

Вы можете настроить уведомления о событии позднее без запуска мастера первоначальной настройки.

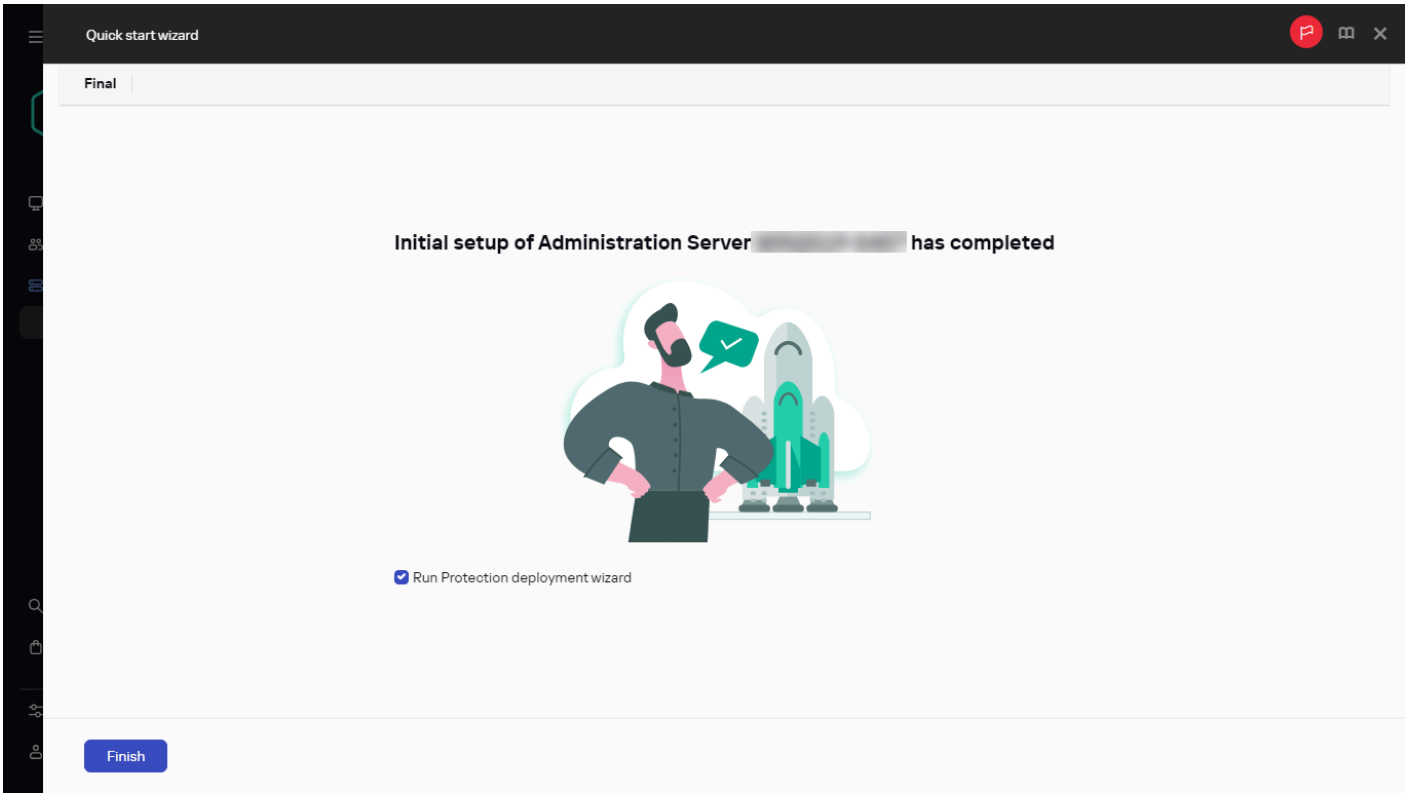
Шаг 13. Выполнение опроса сети

Сервер администрирования выполняет первоначальный опрос сети. Во время опроса отображается ход его выполнения. После завершения опроса ссылка **Просмотреть обнаруженные устройства** становится доступной. Вы можете перейти по ссылке, чтобы просмотреть устройства сети, обнаруженные Сервером администрирования. Чтобы вернуться в мастер первоначальной настройки, нажмите на кнопку **Escape**.

Вы можете выполнить опрос сети позднее без запуска мастера первоначальной настройки. С помощью Kaspersky Security Center Web Console настройте опрос контроллеров домена, Windows-доменов, IP-диапазонов и IPv6-сетей.

Шаг 14. Завершение работы мастера первоначальной настройки

На странице завершения работы мастера первоначальной настройки установите флажок **Запустить мастер развертывания защиты на рабочих станциях**, если вы хотите запустить автоматическую установку антивирусных приложений или Агента администрирования на устройства в вашей сети.



Последний шаг мастера первоначальной настройки

Для завершения работы мастера нажмите на кнопку **Готово**.

Подключение автономных устройств

В этом разделе описано, как подключить автономные устройства к Серверу администрирования (то есть управляемые устройства, находящиеся вне основной сети).

Сценарий: подключение автономных устройств через шлюз соединения

В этом сценарии описано, как подключить к Серверу администрирования управляемые устройства, находящиеся вне основной сети.

Предварительные требования

Сценарий имеет следующие предварительные требования:

- В сети вашей организации организована демилитаризованная зона (DMZ).
- Сервер администрирования Kaspersky Security Center развернут в корпоративной сети.

Этапы

Этот сценарий состоит из следующих этапов:

1. **Выбор клиентского устройства в демилитаризованной зоне**

   Это устройство будет использоваться в качестве шлюза соединения. Выбранное устройство должно соответствовать требованиям для шлюзов соединения.

2. **Установка Агента администрирования в роли шлюза соединения**

   Для установки Агента администрирования на выбранное устройство рекомендуем использовать локальную установку.

   По умолчанию установочный файл находится по адресу: \\<Имя Сервера>\KLSHARE\PkgInst\NetAgent_<номер версии>.

   В окне **Шлюз соединения** мастера установки Агента администрирования выберите параметр **Использовать в качестве шлюза соединения в демилитаризованной зоне**. Этот режим одновременно активирует роль шлюза соединения и предписывает Агенту администрирования ждать соединений от Сервера администрирования, а не устанавливать соединения с Сервером администрирования.

   Также вы можете установить Агент администрирования на устройство под управлением Linux и настроить Агент администрирования для работы в качестве шлюза соединения. Обратите внимание на список ограничений Агента администрирования, работающего на устройствах под управлением Linux.

3. **Разрешение соединения на сетевом экране шлюза соединения**

   Чтобы Сервер администрирования мог подключаться к шлюзу соединения в демилитаризованной зоне, разрешите подключения к TCP-порту 13000 во всех сетевых экранах между Сервером администрирования и шлюзом соединения.

   Если шлюз соединения не имеет реального IP-адреса в интернете, но вместо этого расположен за Network Address Translation (далее также NAT), настройте правило для пересылки подключений через NAT.

4. **Создание группы администрирования для внешних устройств**

   Создайте группу внутри группы **Управляемые устройства**. Эта новая группа будет содержать внешние управляемые устройства.

5. **Подключение шлюза соединения к Серверу администрирования**

   Настроенный вами шлюз соединения ожидает соединения от Сервера администрирования. Однако Сервер администрирования не перечисляет устройство со шлюзом соединения среди управляемых устройств. Это связано с тем, что шлюз соединения не пытался установить соединение с Сервером администрирования. Следовательно, вам потребуется особая процедура, чтобы Сервер администрирования инициировал соединение со шлюзом соединения.

Выполните следующие действия:

1. Добавьте шлюз соединения в качестве точки распространения.
2. Переместите шлюз соединения из группы **Нераспределенные устройства** в группу, которую вы создали для внешних устройств.

Шлюз соединения подключен и настроен.

6. **Подключение внешних настольных устройств к Серверу администрирования**

   Обычно внешние настольные устройства не перемещаются внутрь периметра сети. Поэтому вам необходимо настроить их для подключения к Серверу администрирования через шлюз соединения при установке Агента администрирования.

7. **Настройка обновлений для внешних настольных устройств**

   Если обновления приложений безопасности настроены на загрузку с Сервера администрирования, внешние устройства загружают обновления через шлюз соединения. Это имеет два недостатка:

   - Это лишний трафик, занимающий пропускную способность интернет-канала компании.
   - Это не обязательно самый быстрый способ получать обновления. Возможно для внешних устройств будет удобнее получать обновления с серверов обновлений "Лаборатории Касперского".

   Выполните следующие действия:

   1. Переместите все внешние устройства в отдельную группу администрирования, которую вы создали ранее.
   2. Исключить группу с внешними устройствами из задачи обновления.
   3. Создайте отдельную задачу обновления для группы с внешними устройствами.

8. **Подключение ноутбуков к Серверу администрирования**

   Иногда ноутбуки находятся внутри сети, а в другое время – вне сети. Для эффективного управления вам необходимо, чтобы они по-разному подключались к Серверу администрирования в зависимости от своего местоположения. Для эффективного использования трафика им также необходимо получать обновления из разных источников в зависимости от их местоположения.

   Вам необходимо настроить правила для автономных пользователей: профили подключения и описания сетевых расположений. Каждое правило определяет экземпляр Сервера администрирования, к которому должны подключаться ноутбуки в зависимости от их местоположения, и экземпляр Сервера администрирования, с которого они должны получать обновления.

Сценарий: подключение автономных устройств через подчиненный Сервер администрирования в демилитаризованной зоне

Если вы хотите подключить управляемые устройства, расположенные вне основной сети, к Серверу администрирования, вы можете сделать это с помощью подчиненного Сервера администрирования, расположенного в демилитаризованной зоне (DMZ).

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- В сети вашей организации организована демилитаризованная зона (DMZ).
- Сервер администрирования Kaspersky Security Center развернут во внутренней сети организации.

Этапы

Этот сценарий состоит из следующих этапов:

1. **Выбор клиентского устройства в демилитаризованной зоне**

   В демилитаризованной зоне (DMZ) выберите клиентское устройство, которое будет использоваться в качестве подчиненного Сервера администрирования.

2. **Установка Сервера администрирования Kaspersky Security Center.**

   Установите Сервер администрирования Kaspersky Security Center на этом клиентском устройстве.

3. **Создание иерархии Серверов администрирования**

   Если вы размещаете подчиненный Сервер администрирования в демилитаризованной зоне, подчиненный Сервер администрирования должен принимать подключение от главного Сервера администрирования. Для этого добавьте новый Сервер администрирования в качестве подчиненного Сервера так, чтобы главный Сервер подключался к подчиненному Серверу по порту 13000. При объединении Серверов в иерархию необходимо, чтобы порт 13299 обоих Серверов был доступен. Приложение Kaspersky Security Center Web Console подключается к Серверу администрирования по порту 13299.

4. **Подключение автономных управляемых устройств к подчиненному Серверу администрирования**

   Вы можете подключить автономные устройства к Серверу администрирования в демилитаризованной зоне аналогично тому, как устанавливается соединение между Сервером администрирования и управляемыми устройствами находящимися в основной сети. Автономные устройства инициируют подключение через порт 13000.

О подключении автономных устройств

Некоторые управляемые устройства, которые всегда находятся вне основной сети (например, устройства в региональных филиалах компании; киоски, банкоматы и терминалы, установленные в различных точках продаж; устройства в домашних офисах сотрудников), не могут быть подключены к Серверу администрирования напрямую. Некоторые устройства время от времени выходят за пределы периметра сети (например, ноутбуки пользователей, которые посещают региональные филиалы или офис клиента).

Вам по-прежнему необходимо отслеживать и управлять защитой устройств вне офиса – получать актуальную информацию об их статусе защиты и поддерживать приложения безопасности на них в актуальном состоянии. Это необходимо, например, потому, что если такое устройство будет скомпрометировано, находясь вдали от основной сети, то оно может стать платформой для распространения угроз, как только подключится к основной сети. Для подключения автономных устройств к Серверу администрирования вы можете использовать два способа:

- Шлюз соединения в демилитаризованной зоне (DMZ).

  См. схему трафика данных: Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете; использование шлюза соединения.

- Сервер администрирования в демилитаризованной зоне (DMZ)

  См. схему трафика данных: Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете.

Шлюз соединения в демилитаризованной зоне

Рекомендуемый способ подключения автономных устройств к Серверу администрирования это создание демилитаризованной зоны в сети организации и установка шлюза соединения в демилитаризованной зоне. Внешние устройства будут подключаться к шлюзу соединения, а Сервер администрирования внутри сети инициирует подключение к устройствам через шлюз соединения.

По сравнению с другим способ этот является более безопасным:

- Вам не нужно открывать доступ к Серверу администрирования извне.
- Скомпрометированный шлюз соединения не представляет большого риска для безопасности сетевых устройств. Шлюз соединения ничем не управляет и не устанавливает никаких соединений.

Кроме того, шлюз соединения не требует много аппаратных ресурсов.

Однако этот способ имеет более сложный процесс настройки:

- Чтобы устройство выполняло роль шлюза соединения в демилитаризованной зоне, вам необходимо установить Агент администрирования и подключить его к Серверу администрирования особым образом.
- Вы не сможете использовать один и тот же адрес подключения к Серверу администрирования для ситуаций. С внешней стороны периметра вам нужно будет использовать не только другой адрес (адрес шлюза соединения), но и другой режим подключения: через шлюз соединения.
- Вам также необходимо определить разные параметры подключения для ноутбуков в разных месторасположениях.

Чтобы добавить шлюз соединения в ранее настроенную сеть:

1. Установите Агент администрирования в режиме шлюза соединения.
2. Переустановите Агент администрирования на устройствах, которые вы хотите подключить к вновь добавленному шлюзу соединения.

Сервер администрирования в демилитаризованной зоне (DMZ)

Другой способ это установка единого Сервера администрирования в демилитаризованной зоне.

Эта конфигурация менее безопасна, чем конфигурация первого способа. В этом случае для управления внешними ноутбуками Сервер администрирования должен принимать соединения с любого адреса из интернета. Сервер администрирования управляет всеми устройствами во внутренней сети, но из демилитаризованной зоны. Поэтому скомпрометированный Сервер может нанести огромный ущерб, несмотря на низкую вероятность такого события.

Риск значительно снижается, если Сервер администрирования в демилитаризованной зоне не управляет устройствами внутренней сети. Такая конфигурация может использоваться, например, поставщиком услуг для управления устройствами клиентов.

Вы можете использовать этот способ в следующих случаях:

- Если вы знакомы с установкой и настройкой Сервера администрирования и не хотите выполнять другую процедуру по установке и настройке шлюза соединения.
- Если вам нужно управлять большим количеством устройств. Максимальное количество устройств, которыми может управлять Сервер администрирования – 100 000 устройств, шлюз соединения может поддерживать до 10 000 устройств.

Это решение также имеет некоторые сложности:

- Серверу администрирования требуется больше аппаратных ресурсов и еще одна база данных.
- Информация об устройствах будет храниться в двух несвязанных между собой базах данных (для Сервера администрирования внутри сети и другой в демилитаризованной зоне), что усложняет контроль.
- Для управления всеми устройствами Сервер администрирования необходимо объединить в иерархию, что усложняет и контроль и управление. Экземпляр подчиненного Сервера администрирования накладывает ограничения на возможные структуры групп администрирования. Вам нужно решить, как и какие задачи и политики распространять на подчиненный Сервер администрирования.
- Настройка внешних устройств для использования Сервера администрирования в демилитаризованной зоне извне и для использования главного Сервера администрирования изнутри не проще, чем настройка подключения через шлюз.
- Высокие риски безопасности. Скомпрометированный Сервер администрирования упрощает взлом управляемых ноутбуков. Если это произойдет, хакерам просто нужно дождаться, пока один из ноутбуков вернется в корпоративную сеть, чтобы продолжить атаку на локальную сеть.

Подключение внешних настольных устройств к Серверу администрирования

Настольные устройства, которые всегда находятся вне основной сети (например, устройства в региональных филиалах компании; киоски, банкоматы и терминалы, установленные в различных точках продаж; устройства в домашних офисах сотрудников), не могут быть подключены к Серверу администрирования напрямую. Они должны быть подключены к Серверу администрирования через шлюз соединения, установленный в демилитаризованной зоне (DMZ). Такая конфигурация выполняется при установке Агента администрирования на эти устройства.

Подключение внешних настольных устройств к Серверу администрирования

1. Создание инсталляционного пакета Агента администрирования.
2. Откройте свойства созданного инсталляционного пакета, перейдите в раздел **Параметры** → **Дополнительно** и выберите параметр **Подключаться к Серверу администрирования через шлюз соединения**.

   Параметр **Подключаться к Серверу администрирования через шлюз соединения** несовместим с параметром **Использовать в качестве шлюза соединения в демилитаризованной зоне**. Вы не можете включить оба этих параметра одновременно.

3. Укажите адрес шлюза соединения в поле **Адрес шлюза соединения**.

   Если шлюз соединения расположен за Network Address Translation (NAT) и не имеет собственного общедоступного адреса, настройте правило шлюза NAT для перенаправления соединений с общедоступного адреса на внутренний адрес шлюза соединения.

4. Создайте автономный инсталляционный пакет на основе созданного инсталляционного пакета.
5. Доставьте автономный инсталляционный пакет на целевые устройства в электронном виде или на съемном диске.
6. Установите Агент администрирования из автономного инсталляционного пакета.

К Серверу администрирования подключены внешние настольные устройства.

О профилях соединения для автономных пользователей

При работе автономных пользователей, использующих ноутбуки (далее также "устройства"), может понадобиться изменить способ подключения к Серверу администрирования или переключиться между Серверами администрирования в зависимости от текущего положения устройства в сети.

Профили подключения поддерживаются только для устройств под управлением Windows и macOS.

Использование различных адресов одного и того же Сервера администрирования

Устройства с установленным Агентом администрирования могут в разные периоды времени подключаться к Серверу администрирования как из внутренней сети организации, так и из интернета. В этой ситуации может потребоваться, чтобы Агент администрирования использовал различные адреса для подключения к Серверу администрирования: внешний адрес Сервера при подключении из интернета и внутренний адрес Сервера при подключении из внутренней сети.

Для этого в свойствах политики Агента администрирования добавьте профиль для подключения к Серверу администрирования из интернета (в разделе **Параметры приложения → Подключения → Профили соединений → Профили подключения к Серверу администрирования**). В окне создания профиля выключите параметр **Использовать только для получения обновлений** и убедитесь, что выбран параметр **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**. Если для доступа к Серверу администрирования используется шлюз соединений (например, в конфигурации Kaspersky Security Center, описанной в разделе Доступ из интернета: Агент администрирования в качестве шлюза соединения в демилитаризованной зоне), в профиле подключения следует указать адрес шлюза соединения в соответствующем поле.

Переключение между Серверами администрирования в зависимости от текущей сети

Если в организации несколько офисов с различными Серверами администрирования и между ними перемещается часть устройств с установленным Агентом администрирования, то необходимо, чтобы Агент администрирования подключался к Серверу администрирования локальной сети того офиса, в котором находится устройство.

В этом случае в свойствах политики Агента администрирования создайте профиль подключения к Серверу администрирования для каждого из офисов, за исключением домашнего офиса, в котором расположен исходный домашний Сервер администрирования. В профилях подключения укажите адреса соответствующих Серверов администрирования и включите (либо выключите) параметр **Использовать только для получения обновлений**:

- выбрать параметр, если требуется, чтобы Агент администрирования синхронизировался с домашним Сервером администрирования, а локальный Сервер использовался только для загрузки обновлений;
- выключить параметр, если необходимо, чтобы Агент администрирования полностью управлялся локальным Сервером администрирования.

Далее необходимо настроить условия переключения на созданные профили: не менее одного условия для каждого из офисов, исключая "домашний офис". Смысл каждого такого условия заключается в обнаружении в сетевом окружении деталей, присущих одному из офисов. Если условие становится истинным, происходит активация соответствующего профиля. Если ни одно из условий не является истинным, Агент администрирования переключается на домашний Сервер администрирования.

Создание профиля соединения для автономных пользователей

Подключение профиля Агента администрирования к Серверу администрирования доступно только для устройств под управлением операционной системы Windows и macOS.

Чтобы создать профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей:

1. Если вы хотите создать профиль подключения для группы управляемых устройств, откройте политику Агента администрирования этой группы. Для этого выполните следующие:
   a. В главном окне приложения перейдите в раздел **Активы (Устройства) → Политики и профили политик**.
   b. Перейдите по ссылке на текущий путь.

c. В открывшемся окне выберите нужную группу администрирования.

После этого текущий путь меняется.

d. Добавьте политику Агента администрирования для группы управляемых устройств. Если вы уже создали ее, нажмите на название политики Агента администрирования, чтобы открыть свойства политики.

2. Если вы хотите создать профиль подключения для определенного управляемого устройства, выполните следующие действия:

a. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.

b. Нажмите на имя требуемого управляемого устройства.

c. В открывшемся окне свойств управляемого устройства перейдите на вкладку **Приложения**.

d. Нажмите на название политики Агента администрирования, к которой применяется только выбранное управляемое устройство.

3. В открывшемся окне свойств перейдите в раздел **Параметры приложения** → **Подключения** → **Профили соединений.**

4. В разделе **Профили подключения к Серверу администрирования** нажмите на кнопку **Добавить**.

По умолчанию список профилей подключения содержит профили <Офлайн-режим> и <Домашний Сервер администрирования>. Профили недоступны для изменения и удаления.

В профиле <Офлайн-режим> не указывается Сервер для подключения. При переходе к этому профилю Агент администрирования не пытается подключиться к какому-либо Серверу, а установленные на клиентских устройствах приложения используют политики для автономных пользователей. Профиль <Офлайн-режим> применяется в условиях отключения устройств от сети.

В профиле <Домашний Сервер администрирования> указан Сервер для подключения, который был задан при установке Агента администрирования. Профиль <Домашний Сервер администрирования> применяется в условиях, когда устройство, которое работало в другой сети, вновь подключается к домашнему Серверу администрирования.

5. В открывшемся окне **Настроить профиль** настройте параметры профиля подключения:

- **Имя профиля**

  В поле ввода можно просмотреть или изменить имя профиля подключения.

- **Адрес Сервера администрирования**

  Адрес Сервера администрирования, к которому должно подключаться клиентское устройство при активации профиля.

- **Номер порта**

  Номер порта, по которому будет выполняться подключение.

- **SSL-порт**

  Номер порта, по которому будет осуществляться подключение с использованием SSL-протокола.

- **Использовать SSL-соединение**

  Если этот параметр включен, подключение будет выполняться через защищенный порт (с использованием SSL-протокола).

  По умолчанию параметр включен. Чтобы ваше соединение оставалось безопасным, рекомендуется не выключать этот параметр.

- Выберите параметр **Использовать прокси-сервер**, если требуется использовать прокси-сервер для подключения к интернету. Если параметр выбран, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

  - **Адрес**

    Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.

  - **Номер порта**

    Номер порта, через который будет установлено прокси-подключение Kaspersky Security Center.

  - **Аутентификация на прокси-сервере**

    Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  - **Имя пользователя**

    Учетная запись пользователя, от имени которого будет выполняться подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

  - **Пароль**

    Пароль пользователя, с помощью учетной записи которого выполняется подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

    Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

- **Адрес шлюза соединения**

  Адрес шлюза, через который устанавливается соединение клиентских устройств с Сервером администрирования.

- **Включить автономный режим, когда Сервер администрирования недоступен**

  Установите этот флажок, чтобы при подключении приложения, установленные на клиентском устройстве, использовали профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей, если Сервер администрирования недоступен. В случае, если для приложения политика для автономных пользователей не определена, приложение будет использовать активную политику.

  Если параметр выключен, приложения будут использовать активные политики.

  По умолчанию флажок снят.

- **Использовать только для получения обновлений**

  Если этот параметр включен, профиль будет использоваться только при загрузке обновлений приложениями, установленными на клиентском устройстве. Для остальных операций подключение к Серверу администрирования будет выполняться с исходными параметрами подключения, заданными при установке Агента администрирования.

По умолчанию параметр включен.

- **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**

  Если этот параметр включен, Агент администрирования подключается к Серверу администрирования, используя параметры, указанные в свойствах профиля.

  Если этот параметр выключен, Агент администрирования подключается к Серверу, используя исходные параметры, указанные при установке.

  Параметр доступен, если параметр **Использовать только для получения обновлений** выключен.

  По умолчанию параметр выключен.

В результате будет создан профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей. При подключении Агента администрирования к Серверу через этот профиль приложения, установленные на клиентском устройстве, будут использовать политики для устройств, находящиеся в автономном режиме, или политики для автономных пользователей.

О переключении Агента администрирования на другой Сервер администрирования

В Kaspersky Security Center предусмотрена возможность переключать Агент администрирования клиентского устройства на другие Серверы администрирования при изменении следующих характеристик сети:

- **Условие для адреса DHCP-сервера** – изменение IP-адреса DHCP-сервера (Dynamic Host Configuration Protocol) в сети.
- **Условие для адреса шлюза соединения по умолчанию** – изменение основного шлюза сети.
- **Условие для DNS-домена** – изменение DNS-суффикса подсети.
- **Условие для адресов DNS-сервера** – изменение IP-адреса DNS-сервера в сети.
- **Условие для адреса WINS-сервера** – изменение IP-адреса WINS-сервера в сети. Этот параметр доступен только для устройств с операционными системами Windows.
- **Условие для разрешимости имен** – у клиентского устройства изменилось NetBIOS-имя или DNS-имя.
- **Условие для подсети** – изменение адреса и маски подсети.
- **Условие для доступности Windows-домена** – изменение статуса Windows-домена, к которому подключено клиентское устройство. Этот параметр доступен только для устройств с операционными системами Windows.
- **Условие для доступности адреса SSL-соединения** – клиентское устройство может или не может (в зависимости от выбранного вами параметра) установить SSL-соединение с сервером (имя:порт). Следует использовать выделенный сервер с программным обеспечением, способным работать под высокой нагрузкой и обрабатывать частые запросы соединения от Агента администрирования. Не указывайте порт Сервера администрирования. Для каждого сервера вы можете дополнительно указать SSL-сертификат. В этом случае Агент администрирования проверяет сертификат сервера в дополнение к проверке возможности SSL-соединения. Если сертификаты не совпадают, соединение не устанавливается.

Эта функция поддерживается только для Агентов администрирования, установленных на устройствах под управлением Windows или macOS.

Исходные параметры подключения Агента администрирования к Серверу задаются при установке Агента администрирования. В дальнейшем, если сформированы правила переключения Агента администрирования на другие Серверы администрирования, Агент реагирует на изменение характеристик сети следующим образом:

- Если характеристики сети соответствуют одному из сформированных правил, Агент администрирования подключается к указанному в этом правиле Серверу администрирования. Если это задано правилом, установленные на клиентских устройствах приложения переходят на политики для автономных пользователей.

- Если ни одно из правил не выполняется, Агент администрирования возвращается к исходным параметрам подключения к Серверу администрирования, заданным при установке. Установленные на клиентских устройствах приложения возвращаются к активным политикам.

- Если Сервер администрирования недоступен, Агент администрирования использует политики для автономных пользователей.

Агент администрирования переключается на политику для автономных пользователей, только если параметр **Включить автономный режим, когда Сервер администрирования недоступен** включен в параметрах политики Агента администрирования.

Параметры подключения Агента администрирования к Серверу администрирования сохраняются в профиле подключения. В профиле подключения вы можете создавать правила перехода клиентских устройств на политики для автономных пользователей, а также настраивать профиль таким образом, чтобы он использовался только для загрузки обновлений.

Создание правила переключения Агента администрирования по сетевому местоположению

Переключение Агента администрирования доступно только для устройств под управлением операционной системы Windows и macOS.

Чтобы создать правило для переключения Агента администрирования с одного Сервера администрирования на другой при изменении характеристик сети:

1. Если вы хотите создать правило для группы управляемых устройств, откройте политику Агента администрирования этой группы. Для этого выполните следующие:

   a. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.

   b. Перейдите по ссылке на текущий путь.

   c. В открывшемся окне выберите нужную группу администрирования.

      После этого текущий путь меняется.

   d. Добавьте политику Агента администрирования для группы управляемых устройств. Если вы уже создали ее, нажмите на название политики Агента администрирования, чтобы открыть свойства политики.

2. Если вы хотите создать правило для определенного управляемого устройства, сделайте следующее:

   a. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.

   b. Нажмите на имя требуемого управляемого устройства.

   c. В открывшемся окне свойств управляемого устройства перейдите на вкладку **Приложения**.

   d. Нажмите на название политики Агента администрирования, к которой применяется только выбранное управляемое устройство.

3. В открывшемся окне свойств перейдите в раздел **Параметры приложения** → **Подключения** → **Профили соединений.**

4. В разделе **Параметры сетевого местоположения** нажмите на кнопку **Добавить**.

5. В открывшемся окне свойств настройте описание сетевого местоположения и правило переключения. Настройте следующие параметры описания сетевого местоположения:

   - **Описание**

     Имя описания сетевого местоположения не может превышать 255 символов и содержать специальные символы ("*<>?\/:|).

   - **Использовать профиль подключения**

     В раскрывающемся списке можно выбрать профиль подключения Агента администрирования к Серверу администрирования. Профиль будет использоваться при выполнении условий описания сетевого местоположения. Профиль подключения содержит параметры подключения Агента администрирования к Серверу администрирования и определяет переход клиентских устройств на политики для автономных пользователей. Профиль используется только для загрузки обновлений.

   - **Описание активно**

     Установите этот флажок, чтобы включить использование нового описания сетевого местоположения.

6. Выберите условия для правила переключения Агента администрирования:

   - **Условие для адреса DHCP-сервера** – изменение IP-адреса DHCP-сервера (Dynamic Host Configuration Protocol) в сети.

   - **Условие для адреса шлюза соединения по умолчанию** – изменение основного шлюза сети.

   - **Условие для DNS-домена** – изменение DNS-суффикса подсети.

   - **Условие для адресов DNS-сервера** – изменение IP-адреса DNS-сервера в сети.

   - **Условие для адреса WINS-сервера** – изменение IP-адреса WINS-сервера в сети. Этот параметр доступен только для устройств с операционными системами Windows.

   - **Условие для разрешимости имен** – у клиентского устройства изменилось NetBIOS-имя или DNS-имя.

   - **Условие для подсети** – изменение адреса и маски подсети.

- **Условие для доступности Windows-домена** – изменение статуса Windows-домена, к которому подключено клиентское устройство. Этот параметр доступен только для устройств с операционными системами Windows.

- **Условие для доступности адреса SSL-соединения** – клиентское устройство может или не может (в зависимости от выбранного вами параметра) установить SSL-соединение с Сервером (имя:порт). Для каждого сервера вы можете дополнительно указать SSL-сертификат. В этом случае Агент администрирования проверяет сертификат Сервера администрирования в дополнение к проверке возможности SSL-соединения. Если сертификаты не совпадают, соединение не устанавливается.

Условия правила объединяются с использованием логического оператора AND. Чтобы правило переключения по описанию сетевого местоположения сработало, все условия переключения правила должны быть выполнены.

7. В разделе с условиями укажите, когда Агент администрирования нужно переключить на другой Сервер администрирования. Для этого нажмите на кнопку **Добавить** и установите значение условия.

   Параметр **Соответствует хотя бы одному значению списка** включен по умолчанию. Можно выключить этот параметр, если вы хотите, чтобы условие выполнялось со всеми указанными значениями.

8. Сохраните изменения.

В результате будет создано правило переключения по описанию сетевого местоположения, при выполнении условий которого Агент администрирования будет использовать для подключения к Серверу администрирования указанный в описании профиль подключения.

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**.

Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat, чтобы настроить Агент администрирования.

Шаг 1. Запуск мастера развертывания защиты

Чтобы запустить мастер развертывания защиты вручную,

В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Мастер развертывания защиты**.

Запустится мастер развертывания защиты. Для продолжения работы мастера нажмите на кнопку **Далее**.

Шаг 2. Выбор инсталляционного пакета

Выберите инсталляционный пакет приложения, которое требуется установить.

Если инсталляционный пакет требуемого приложения не содержится в списке, нажмите на кнопку **Добавить** и выберите приложение из списка.

Шаг 3. Выбор способа распространения файла ключа или кода активации

Выберите способ распространения файла ключа или кода активации:

- **Не добавлять лицензионный ключ в инсталляционный пакет**

  Если выбран этот вариант, ключ будет автоматически распространяться на те устройства, для которых он подходит:

  - если в свойствах ключа настроено автоматическое распространение;
  - если создана задача **Добавление ключа**.

- **Добавить лицензионный ключ в инсталляционный пакет**

  Ключ распространяется на устройства вместе с инсталляционным пакетом.

  > Не рекомендуется распространять ключ таким способом, так как по умолчанию к хранилищу инсталляционных пакетов настроен общий доступ на чтение.

Если инсталляционный пакет уже содержит файл ключа или код активации, это окно отображается, но оно содержит только информацию о лицензионном ключе.

Шаг 4. Выбор версии Агента администрирования

Если вы выбрали инсталляционный пакет приложения, отличный от Агента администрирования, необходимо также установить Агент администрирования для подключения приложения к Серверу администрирования Kaspersky Security Center.

Выберите последнюю версию Агента администрирования.

Шаг 5. Выбор устройств

Укажите список устройств, на которые требуется установить приложение:

- **Установить на управляемые устройства**

  Если выбран этот вариант, задача удаленной установки приложения будет создана для группы устройств.

- **Выбор устройств для установки**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

Шаг 6. Задание параметров задачи удаленной установки

В окне **Параметры задачи удаленной установки** настройте параметры удаленной установки приложения.

В блоке параметров **Принудительно загрузить инсталляционный пакет** выберите способ доставки на клиентские устройства файлов, необходимых для установки приложения:

- **С помощью Агента администрирования**

  Если этот параметр включен, доставку инсталляционных пакетов на клиентские устройства выполняет установленный на клиентских устройствах Агент администрирования.

  Если этот параметр выключен, инсталляционные пакеты доставляются с помощью инструментов операционной системы клиентского устройства.

  Рекомендуется включить этот параметр, если задача назначена для устройств с установленными Агентами администрирования.

  По умолчанию параметр включен.

- **Средствами операционной системы с помощью точек распространения**

  Если флажок установлен, инсталляционные пакеты передаются на клиентские устройства средствами операционной системы через агенты обновлений. Этот вариант можно выбрать, если в сети есть хотя бы один агент обновлений.

Если установлен флажок **С помощью Агента администрирования**, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

По умолчанию флажок установлен для задач удаленной установки, созданных на виртуальном Сервере администрирования.

Единственный способ установить приложение для Windows (включая Агент администрирования для Windows) на устройство, на котором не установлен Агент администрирования, – это использовать точку распространения с операционной системой Windows. Поэтому при установке приложения для Windows:

- Выберите этот параметр.
- Убедитесь, что для целевых клиентских устройств назначена точка распространения.
- Убедитесь, что на точке распространения установлена операционная система Windows.

- **Средствами операционной системы с помощью Сервера администрирования**

  Если этот параметр включен, доставка файлов на клиентские устройства будет осуществляться средствами операционной системы клиентских устройств с помощью Сервера администрирования. Этот параметр можно включить, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

  По умолчанию параметр включен.

Настройте 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.

- **Назначить установку инсталляционного пакета в групповых политиках Active Directory**

  Если этот параметр включен, инсталляционный пакет будет устанавливаться с помощью групповых политик Active Directory.

  Параметр доступен, если выбран инсталляционный пакет Агента администрирования.

  По умолчанию параметр выключен.

Шаг 7. Управление перезагрузкой

Укажите действие, которое требуется выполнить, если необходимо перезагрузить операционную систему во время установки приложения:

- **Не перезагружать устройство**

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

  - **Повторять запрос каждые (мин)**

    Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

    По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

    Если параметр выключен, предложение перезагрузки отображается только один раз.

  - **Принудительно перезагрузить через (мин)**

    После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

    По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать приложения в заблокированных сеансах**

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.

Шаг 8. Удаление несовместимых приложений перед установкой

Этот шаг присутствует, только если приложение, которое вы разворачиваете, несовместимо с другими приложениями.

Выберите этот параметр, если вы хотите, чтобы приложение Kaspersky Security Center автоматически удаляло несовместимые приложения с приложением, которое вы устанавливаете.

Отображается список несовместимых приложений.

Если этот параметр не выбран, приложение будет установлено только на устройствах, на которых нет несовместимых приложений.

Шаг 9. Перемещение устройств в папку Управляемые устройства

Укажите, следует ли перемещать устройства в группу администрирования после установки Агента администрирования.

- **Не перемещать устройства**

  Устройства остаются в тех группах, к которым они принадлежат. Устройства, не принадлежащие ни к одной из групп, остаются нераспределенными.

- **Перемещать нераспределенные устройства в группу**

  Устройства перемещаются в выбранную вами группу администрирования.

По умолчанию выбран вариант **Не перемещать устройства**. По соображениям безопасности вы можете предпочесть перемещение устройств вручную.

Шаг 10. Выбор учетных записей для доступа к устройствам

Если необходимо, добавьте учетные записи, которые будут использоваться для запуска задачи удаленной установки:

- **Учетная запись не требуется (Агент администрирования уже установлен)**

  Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор приложения. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

  Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

- **Учетная запись требуется (Агент администрирования не используется)**

  Выберите этот вариант, если Агент администрирования не установлен на устройствах, для которых вы назначаете задачу удаленной установки. В этом случае вы можете указать учетную запись пользователя или SSH-сертификат для установки приложения.

  - **Локальная учетная запись**. Если выбран этот вариант, укажите учетную запись пользователя, от имени которой будет запускаться установщик приложения. Нажмите на кнопку **Добавить**, выберите **Локальная учетная запись** и укажите данные учетной записи пользователя.

    Вы можете указать несколько учетных записей, если ни одна из них не обладает необходимыми правами на всех устройствах, для которых назначена задача. В этом случае для запуска задачи используются последовательно, сверху вниз, все добавленные учетные записи.

  - **SSH сертификат**. Если вы хотите установить 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 поддерживает формат закрытых ключей PEM, а утилита ssh-keygen по умолчанию генерирует SSH-ключи в формате OPENSSH. Формат OPENSSH не поддерживается Kaspersky Security Center. Чтобы создать закрытый ключ в поддерживаемом формате PEM, добавьте параметр -m PEM в команду ssh-keygen. Например:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<электронная почта пользователя>"
```

Шаг 11. Запуск установки

Это последний шаг мастера. На этом шаге **Задача удаленной установки приложения** была успешно создана и настроена.

По умолчанию вариант **Запустить задачу после завершения работы мастера** не выбран. Если вы выберете этот параметр, **Задача удаленной установки приложения** начнется сразу после завершения работы мастера. Если вы не выберете этот параметр, **Задача удаленной установки приложения** не начнется. Вы можете запустить эту задачу в дальнейшем вручную.

Нажмите на кнопку **OK**, чтобы завершить последний шаг мастера развертывания защиты.

Развертывание приложений "Лаборатории Касперского" с помощью Kaspersky Security Center Web Console

В этом разделе описано, как развернуть приложения "Лаборатории Касперского" на клиентских устройствах в вашей организации с помощью Kaspersky Security Center Web Console.

Сценарий: развертывание приложений "Лаборатории Касперского" с помощью Kaspersky Security Center Web Console

В этом сценарии описана процедура развертывания приложений "Лаборатории Касперского" с помощью Kaspersky Security Center Web Console. Можно либо воспользоваться мастером первоначальной настройки и мастером развертывания защиты, либо выполнить все необходимые шаги вручную.

Следующие приложения доступны для развертывания с помощью Kaspersky Security Center Web Console:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux

Этапы

Развертывание приложений "Лаборатории Касперского" состоит из следующих этапов:

1. **Загрузка плагина управления приложения.**

   Этот этап обрабатывается мастером первоначальной настройки. Если вы не запускали мастер первоначальной настройки, загрузите плагин для Kaspersky Endpoint Security для Windows вручную.

   Если вы планируете управлять корпоративными мобильными устройствами, следуйте инструкциям в справке Kaspersky Security для мобильных устройств, чтобы загрузить и установить плагины управления Kaspersky Endpoint Security для Android.

2. **Загрузка и создание инсталляционных пакетов**

   Этот этап обрабатывается мастером первоначальной настройки.

   Мастер первоначальной настройки позволяет загрузить инсталляционный пакет совместно с плагином управления. Если вы не выбрали этот параметр при запуске мастера или не запускали мастер, требуется загрузить инсталляционный пакет вручную.

   Если вы не можете установить приложения "Лаборатории Касперского" с помощью Kaspersky Security Center на некоторых устройствах, например, на устройствах удаленных сотрудников, вы можете создавать автономные установочные пакеты для приложений. Если вы используете автономные пакеты для установки приложений "Лаборатории Касперского", вам не нужно создавать и запускать задачу удаленной установки, а также создавать и настраивать задачи для Kaspersky Endpoint Security для Windows.

3. **Создание, настройка и запуск задачи удаленной установки**

   Для Kaspersky Endpoint Security для Windows, этот этап входит в мастер развертывания защиты, который запускается автоматически после завершения мастера первоначальной настройки. Если вы не запускали мастер развертывания защиты, вам необходимо создать и настроить эту задачу вручную.

   Вы можете вручную создать несколько задач удаленной установки для различных групп администрирования или выборок устройств. Вы можете развернуть различные версии одного приложения в этих задачах.

   Убедитесь, что все устройства в сети обнаружены, а затем запустите задачу (или задачи) удаленной установки.

   Установите утилиту nmap на свои Linux-активы. Эта утилита необходима для включения функциональности Network Location Awareness.

   Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat, чтобы настроить Агент администрирования.

   Если вы хотите установить Агент администрирования на устройства с операционной системой РЕД ОС 7.3.4 или выше либо МСВСфера 9.2 или выше, установите пакет libxcrypt-compat для корректной работы Агента администрирования.

4. **Создание и настройка задач для управляемого приложения**

   Задача *Установка обновлений* Kaspersky Endpoint Security для Windows должна быть настроена.

Этот этап входит в мастер первоначальной настройки: задача создается и настраивается автоматически, с параметрами по умолчанию. Если вы не запускали мастер первоначальной настройки, вам необходимо создать и настроить эту задачу вручную. Если вы запускали мастер первоначальной настройки, убедитесь, что расписание запуска задачи соответствует вашим требованиям. (По умолчанию для времени запуска задачи установлено значение **Вручную**, но вам может понадобиться изменить это значение.)

Для других приложений "Лаборатории Касперского" могут существовать другие задачи по умолчанию. Дополнительную информацию см. в документации к соответствующим приложениям.

Убедитесь, что расписание запуска каждой созданной вами задачи соответствует вашим требованиям.

5. **Установка Kaspersky Security для мобильных устройств (необязательно)**

   Если вы планируете управлять корпоративными мобильными устройствами, см. справку Kaspersky Security для мобильных устройств информацию о развертывании Kaspersky Endpoint Security для Android.

6. **Создание политик**

   Создайте политику для каждого приложения вручную или (в случае если вы используете Kaspersky Endpoint Security для Windows) с помощью мастера первоначальной настройки. Можно использовать установленные по умолчанию параметры политики. Также вы можете в любое время изменить заданные по умолчанию параметры политики в соответствии с вашими требованиями.

7. **Проверка результатов**

   Убедитесь, что развертывание завершилось успешно: созданы политики и задачи для каждого приложения и эти приложения установлены на управляемые устройства.

Результаты

Завершение сценария дает следующее:

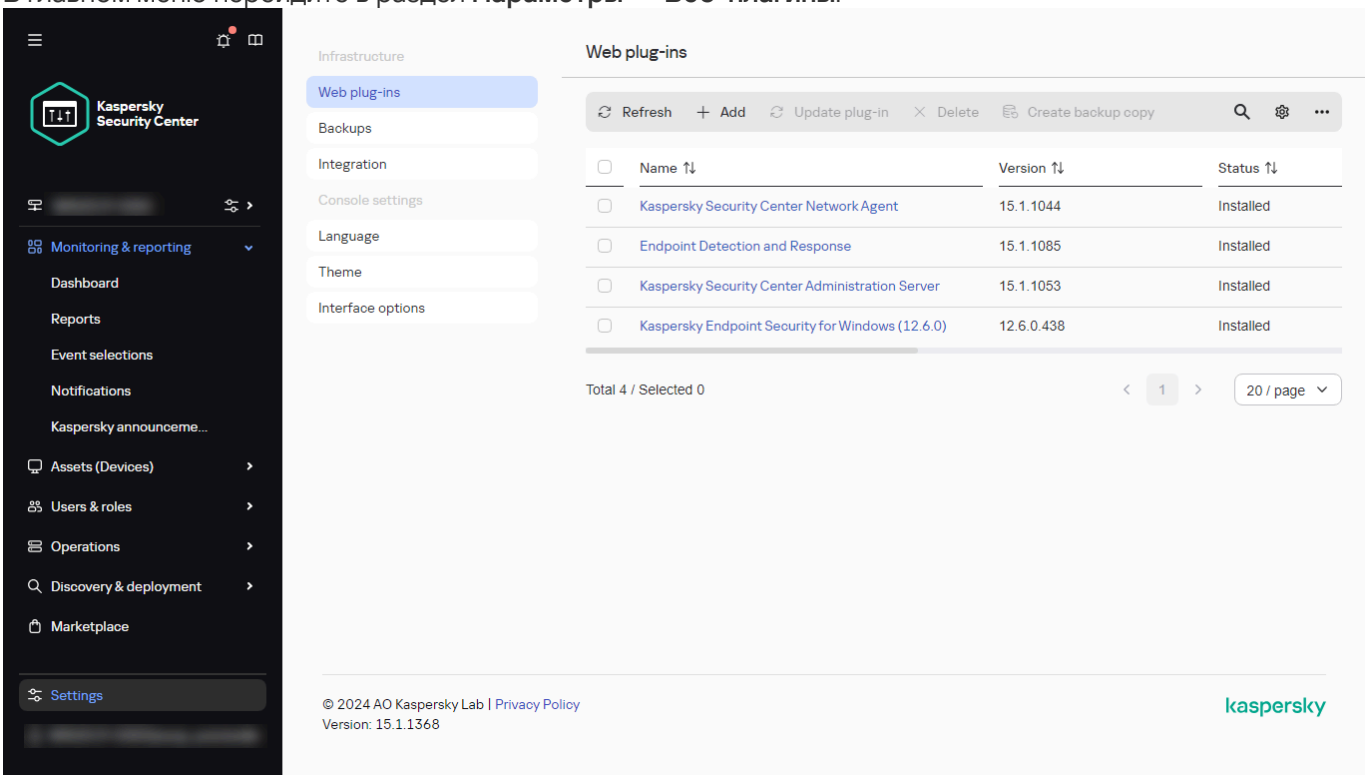
- Все требуемые политики и задачи для выбранных приложений созданы.
- Расписание запуска задач настроено в соответствии с вашими требованиями.
- На выбранных клиентских устройствах развернуты или запланированы к развертыванию выбранные приложения.

Загрузка плагинов для приложений "Лаборатории Касперского"

Для развертывания приложений "Лаборатории Касперского", таких как Kaspersky Endpoint Security для Windows, необходимо загрузить плагины управления для этих приложений.

Чтобы загрузить плагин управления для приложения "Лаборатории Касперского":

1. В главном меню перейдите в раздел **Параметры** → **Веб-плагины**.



Список установленных веб-плагинов

2. В появившемся окне нажмите на кнопку **Добавить**.

   Отобразится список доступных плагинов управления.

3. В списке доступных плагинов выберите имя плагина, который требуется загрузить (например, Kaspersky Endpoint Security 11 для Windows).

   Отобразится страница с описанием плагина.

4. На странице описания плагина нажмите на кнопку **Установить плагин**.

5. После завершения установки нажмите на кнопку **OK**.

Плагин управления будет загружен в конфигурации по умолчанию и появится в списке плагинов управления.

Вы можете добавлять плагины и обновлять загруженные плагины из файла. Вы можете загрузить плагины управления и веб-плагины управления с сайта Службы технической поддержки "Лаборатории Касперского".

Чтобы загрузить или обновить плагин из файла:

1. В главном меню перейдите в раздел **Параметры** → **Веб-плагины**.

2. Выполните одно из следующих действий:

   - Нажмите на **Добавить из файла**, чтобы загрузить плагин из файла.
   - Нажмите на **Обновить из файла**, чтобы загрузить обновление для плагина из файла.

3. Укажите файл и подпись файла.

4. Загрузите указанные файлы.

Плагин управления будет загружен из файла и появится в списке плагинов управления.

Загрузка и создание инсталляционных пакетов для приложений "Лаборатории Касперского"

Если у Сервера администрирования есть доступ в интернет, вы можете создавать инсталляционные пакеты для приложений "Лаборатории Касперского" с веб-серверов "Лаборатории Касперского".

Чтобы загрузить и создать инсталляционный пакет для приложения "Лаборатории Касперского":

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание → Развертывание и назначение → Инсталляционные пакеты**.
   - В главном окне приложения перейдите в раздел **Операции → Хранилища → Инсталляционные пакеты**.

   Вы также можете просматривать информацию о новых пакетах для приложений "Лаборатории Касперского" в списке экранных уведомлений. Если есть уведомления о новом пакете, вы можете перейти по ссылке рядом с уведомлением к списку доступных инсталляционных пакетов.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Выберите **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**.

   Отобразится список инсталляционных пакетов доступных на веб-серверах "Лаборатории Касперского". Список содержит инсталляционные пакеты только тех приложений, которые совместимы с текущей версией Kaspersky Security Center.

4. Выберите требуемый инсталляционный пакет, например, Kaspersky Endpoint Security для Windows (11.1.0).

   Откроется окно с информацией об инсталляционном пакете.

   Вы можете загрузить и использовать инсталляционный пакет, который включает в себя криптографические инструменты, реализующие надежное шифрование, если он соответствует применимым законам и правилам. Чтобы загрузить инсталляционный пакет Kaspersky Endpoint Security для Windows, действительный для нужд вашей организации, обратитесь к законодательству страны, в которой расположены клиентские устройства вашей организации.

5. Ознакомьтесь с информацией и нажмите на кнопку **Загрузить и создать инсталляционный пакет**.

   Если дистрибутив не может быть преобразован в инсталляционный пакет, вместо кнопки **Загрузить и создать инсталляционный пакет** отображается кнопка **Загрузить дистрибутив**.

Начинается загрузка инсталляционного пакета на Сервер администрирования. Вы можете закрыть окно мастера или перейти к следующему шагу инструкции. Если вы закроете мастер, процесс загрузки продолжится в фоновом режиме.

Если вы хотите отслеживать процесс загрузки инсталляционного пакета:

a. В главном окне приложения перейдите в раздел **Операции** → **Хранилища** → **Инсталляционные пакеты** → **В процессе ()**.

b. Следите за ходом операции в графах **Ход загрузки** и **Состояние загрузки** таблицы.

После завершения процесса инсталляционный пакет добавляется в список на вкладке **Загружено**. Если процесс загрузки останавливается и статус загрузки меняется на **Принять Лицензионное соглашение**, нажмите на имя инсталляционного пакета и перейдите к следующему шагу инструкции.

Если размер данных, содержащихся в выбранном дистрибутиве, превышает текущее предельное значение, отображается сообщение об ошибке. Вы можете изменить предельное значение и продолжить создание инсталляционного пакета.

6. Во время процесса загрузки некоторых приложений "Лаборатории Касперского" отображается кнопка **Показать Лицензионное соглашение**. Если эта кнопка отображается:

   a. Нажмите на кнопку **Показать Лицензионное соглашение**, чтобы прочитать Лицензионное соглашение (EULA).

   b. Прочитайте появившееся на экране Лицензионное соглашение и нажмите на кнопку **Принять**.

   Загрузка продолжится после того, как вы примете Лицензионное соглашение. Если вы нажмете на кнопку **Отклонить**, загрузка прекратится.

7. После завершения загрузки нажмите на кнопку **Закрыть**.

Выбранный инсталляционный пакет загружен в папку общего доступа Сервера администрирования, во вложенную папку Packages. После загрузки инсталляционный пакет отображается в списке инсталляционных пакетов.

Изменение ограничения на размер пользовательского инсталляционного пакета

Общий размер данных, распакованных при создании пользовательского инсталляционного пакета, ограничен. Ограничение по умолчанию – 1 ГБ.

Если вы попытаетесь загрузить архивный файл, содержащий данные, превышающие текущее ограничение, появится сообщение об ошибке. Возможно, вам придется увеличить это максимальное значение при создании инсталляционных пакетов из больших дистрибутивов.

Чтобы изменить максимальное значение для размера пользовательского инсталляционного пакета:

1. На устройстве Сервера администрирования запустите командную строку под учетной записью, которая использовалась для установки Сервер администрирования.

2. Измените текущую директорию на папку установки Kaspersky Security Center (обычно это <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).

3. В зависимости от типа установки Сервера администрирования введите одну из следующих команд с правами администратора:

   - Обычная локальная установка:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <число_байтов>
     ```

   - Установка на отказоустойчивый кластер Kaspersky Security Center:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <число_байтов> --stp klfoc
     ```

   - Установка на отказоустойчивый кластер Windows Server:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <число_байтов> --stp
     cluster
     ```

   Где <число_байтов> – количество байтов в шестнадцатеричном или десятичном формате.

   Например, если требуемое максимальное значение составляет 2 ГБ, вы можете указать десятичное значение 2147483648 или шестнадцатеричное значение 0x80000000. В этом случае для локальной установки Сервера администрирования вы можете использовать следующую команду:

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

Ограничение на размер пользовательских данных инсталляционного пакета изменено.

Загрузка дистрибутивов для приложений "Лаборатории Касперского"

В Kaspersky Security Center Web Console вы можете загрузить и сохранить дистрибутив для приложений "Лаборатории Касперского". Вы можете использовать дистрибутивы для установки приложений вручную, без использования Kaspersky Security Center.

Чтобы загрузить и сохранить дистрибутив приложений "Лаборатории Касперского":

1. В главном меню перейдите в раздел **Операции → Приложения "Лаборатории Касперского" → Актуальные версии приложений**.

   Откроется список доступных дистрибутивов, плагинов и патчей. Kaspersky Security Center отображает только те элементы, которые совместимы с его текущей версией приложения.

2. В списке нажмите на имя дистрибутива, который вы хотите загрузить.

   Откроется описание дистрибутива.

3. Ознакомьтесь с описанием и нажмите на кнопку **Загрузить и создать инсталляционный пакет**.

   Если дистрибутив не может быть преобразован в инсталляционный пакет, вместо кнопки **Загрузить дистрибутив** отображается кнопка **Загрузить и создать инсталляционный пакет**.

   Начинается загрузка инсталляционного пакета на Сервер администрирования.

Выбранный инсталляционный пакет или дистрибутив загружен в папку общего доступа Сервера администрирования, во вложенную папку **Packages**. После загрузки инсталляционный пакет отображается в списке инсталляционных пакетов.

Проверка успешности развертывания Kaspersky Endpoint Security

Чтобы убедиться, что вы правильно развернули приложения "Лаборатории Касперского", например, Kaspersky Endpoint Security:

1. С помощью Kaspersky Security Center Web Console проверьте наличие:

   - политики Kaspersky Endpoint Security и/или других приложений безопасности, которые вы используете;
   - задач Kaspersky Endpoint Security для Windows: *Быстрый поиск вирусов* и *Установка обновлений* (если вы используете Kaspersky Endpoint Security для Windows);
   - задач для других приложений безопасности, которые вы используете.

2. Убедитесь, что на управляемых устройствах, для которых была назначена установка:

   - Kaspersky Endpoint Security или другое приложение безопасности "Лаборатории Касперского" установлено;
   - в Kaspersky Endpoint Security параметры Защиты от файловых угроз, Защиты от веб-угроз и Защиты от почтовых угроз соответствуют политике, созданной для этого устройства;
   - можно вручную запустить и остановить службу Kaspersky Endpoint Security;
   - можно вручную запустить и остановить групповые задачи.

Создание автономного инсталляционного пакета

Вы и пользователи устройств в вашей организации можете использовать автономные инсталляционные пакеты для ручной установки приложений на устройства.

Автономный инсталляционный пакет представляет собой исполняемый файл (installer.exe), который можно разместить на Веб-сервере или в общей папке, отправить по почте или передать на клиентское устройство другим способом. Полученный файл можно запустить локально на клиентском устройстве для выполнения установки приложения без участия Kaspersky Security Center. Вы можете создавать автономные инсталляционные пакеты как для приложений "Лаборатории Касперского", так и для приложений сторонних производителей для Windows, macOS и Linux. Чтобы создать автономный инсталляционный пакет для приложений стороннего производителя, необходимо создать пользовательский инсталляционный пакет.

Убедитесь, что автономный инсталляционный пакет не доступен для неавторизованных лиц.

Чтобы создать автономный инсталляционный пакет:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание → Развертывание и назначение → Инсталляционные пакеты**.
   - В главном окне приложения перейдите в раздел **Операции → Хранилища → Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. В списке инсталляционных пакетов выберите пакет и над списком нажмите на кнопку **Развернуть**.

3. Выберите параметр **С использованием автономного инсталляционного пакета**.

   Запустится мастер создания автономного инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. Убедитесь, что включен параметр **Установить Агент администрирования совместно с данным приложением**, если требуется установить Агент администрирования совместно с выбранным приложением.

   Параметр отображается в зависимости от приложения, для которого вы создаете автономный инсталляционный пакет.

   По умолчанию параметр включен. Рекомендуется включить этот параметр, если вы не уверены, установлен ли на устройстве Агент администрирования. Если Агент администрирования уже установлен на устройстве, после установки автономного инсталляционного пакета с Агентом администрирования, Агент администрирования будет обновлен до более новой версии.

   Если вы выключите этот параметр, Агент администрирования не будет установлен на устройство, и устройство не будет управляемым.

   Если автономный инсталляционный пакет для выбранного приложения уже существует на Сервере администрирования, мастер отобразит сообщение об этом. В этом случае вам нужно выбрать одно из следующих действий:

   - **Создать автономный инсталляционный пакет**. Выберите этот параметр, например, если вы хотите создать автономный инсталляционный пакет для новой версии приложения, и чтобы также остался автономный инсталляционный пакет для предыдущей версии приложения, который вы создали ранее. Новый автономный инсталляционный пакет расположен в другой папке.
   - **Использовать существующий автономный инсталляционный пакет**. Выберите этот параметр, если вы хотите использовать существующий автономный инсталляционный пакет. Процесс создания пакета не запускается.
   - **Сформировать заново существующий автономный инсталляционный пакет**. Выберите этот параметр, если хотите создать автономный инсталляционный пакет для этого же приложения еще раз. Автономный инсталляционный пакет размещается в той же папке.

5. На шаге **Перемещение в список управляемых устройств** параметр **Не перемещать устройства** включен по умолчанию. Если вы не хотите перемещать клиентское устройство в какую-либо группу администрирования после установки Агента администрирования, оставьте этот параметр включенным.

   Если вы хотите переместить клиентское устройство после установки Агента администрирования, выберите параметр **Перемещать нераспределенные устройства в эту группу** и укажите группу администрирования, в которую вы хотите переместить клиентское устройство. По умолчанию устройства перемещаются в группу **Управляемые устройства**.

6. После завершения процесса создания автономного инсталляционного пакета, нажмите на кнопку **Готово**.

   Мастер создания автономного инсталляционного пакета закрывается.

Автономный инсталляционный пакет создан и помещен во вложенную папку PkgInst общей папки Сервера администрирования. Вы можете просмотреть список автономных инсталляционных пакетов, нажав на кнопку **Просмотреть список автономных пакетов**, расположенную над списком инсталляционных пакетов.

Просмотр списка автономных инсталляционных пакетов

Вы можете просмотреть список автономных инсталляционных пакетов и свойства каждого отдельного инсталляционного пакета.

Чтобы просмотреть список автономных инсталляционных пакетов для всех инсталляционных пакетов:

Нажмите на кнопку **Просмотреть список автономных пакетов**.

Свойства автономных инсталляционных пакетов в списке отображаются следующим образом:

- **Имя пакета**. Имя автономного инсталляционного пакета, которое автоматически формируется из имени и версии приложения, включенной в пакет.
- **Название приложения**. Имя приложения, которое включено в автономный инсталляционный пакет.
- **Версия приложения**.
- **Имя инсталляционного пакета Агента администрирования**. Параметр отображается только в том случае, если в автономный инсталляционный пакет включен Агент администрирования.
- **Версия Агента администрирования**. Параметр отображается только в том случае, если в автономный инсталляционный пакет включен Агент администрирования.
- **Размер**. Размер файла (МБ).
- **Группа**. Имя группы, в которую перемещается клиентское устройство после установки Агента администрирования.
- **Создан**. Дата и время создания автономного инсталляционного пакета.
- **Изменен**. Дата и время изменения автономного инсталляционного пакета.
- **Путь**. Полный путь к папке, в которой находится автономный инсталляционный пакет.

- **Веб-адрес**. Веб-адрес расположения автономного инсталляционного пакета.
- **Хеш файла**. Параметр используется для подтверждения того, что автономный инсталляционный пакет не был изменен третьими лицами, и у пользователя есть тот же файл, который вы создали и передали пользователю.

Чтобы просмотреть список автономных инсталляционных пакетов для определенного инсталляционного пакета,

выберите инсталляционный пакет в списке и над списком нажмите на кнопку **Просмотреть список автономных пакетов**.

В списке автономных инсталляционных пакетов вы можете сделать следующее:

- Опубликовать автономный инсталляционный пакет на Веб-сервере, с помощью кнопки **Опубликовать**. Опубликованный автономный инсталляционный пакет доступен для загрузки пользователям, которым вы отправили ссылку на автономный инсталляционный пакет.
- Отменить публикацию автономного инсталляционного пакета на Веб-сервере, нажав на кнопку **Отменить публикацию**. Неопубликованный автономный инсталляционный пакет доступен для загрузки только вам и другим администраторам.
- Загрузить автономный инсталляционный пакет на свое устройство, нажав на кнопку **Загрузить**.
- Отправить электронное письмо со ссылкой на автономный инсталляционный пакет, нажав на кнопку **Отправить по электронной почте**.
- Удалить автономный инсталляционный пакет, нажав на кнопку **Удалить**.

Создание пользовательского инсталляционного пакета

Вы можете использовать пользовательские инсталляционные пакеты, чтобы:

- установить любое приложение (такое как текстовый редактор) на клиентские устройства, например, с помощью задачи;
- создать автономный инсталляционный пакет.

Пользовательский инсталляционный пакет – это папка с набором файлов. Источником для создания пользовательского инсталляционного пакета является *архивный файл*. Архивный файл содержит файл или файлы, которые должны быть включены в пользовательский инсталляционный пакет. Во время создания пользовательского инсталляционного пакета, вы можете указать параметры командной строки, например, для установки приложения в тихом режиме.

Если у вас есть активный лицензионный ключ для функции Системного администрирования, вы можете преобразовать параметры установки по умолчанию для соответствующего пользовательского инсталляционного пакета и использовать значения, рекомендованные экспертами "Лаборатории Касперского". Параметры автоматически преобразуются при создании пользовательского инсталляционного пакета, только если соответствующий исполняемый файл включен в базу данных приложений сторонних производителей "Лаборатории Касперского".

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**.

   Откроется стандартное окно Windows **Открыть**, в котором можно выбрать 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) невозможно.

   Если вы хотите, чтобы параметры были преобразованы во время установки пакета, убедитесь, что установлен флажок **Конвертировать параметры на рекомендуемые значения для приложений, распознаваемых Kaspersky Security Center после завершения работы мастера** и нажмите на кнопку **Далее**.

   Начнется загрузка файла на Сервер администрирования Kaspersky Security Center.

   Если вы включили использование рекомендуемых параметров установки, Kaspersky Security Center 15.1 проверяет, включен ли исполняемый файл в базу данных приложений сторонних производителей "Лаборатории Касперского". Если проверка прошла успешно, вы получите уведомление о том, что файл распознан. Параметры сконвертированы и пользовательский инсталляционный пакет создан. Никаких дальнейших действий не требуется. Нажмите на кнопку **Готово**, чтобы закрыть окно мастера.

6. Выберите файл (из списка файлов, которые извлечены из выбранного архивного файла) и укажите параметры командной строки исполняемого файла.

   Вы можете указать параметры командной строки для установки приложения из инсталляционного пакета в тихом режиме. Указывать параметры командной строки необязательно.

   Начнется процесс создания инсталляционного пакета.

   В окне мастера отобразится информация о завершении процесса.

   Если инсталляционный пакет не создан, отобразится соответствующее сообщение.

7. Нажмите на кнопку **Готово**, чтобы закрыть окно мастера.

Созданный инсталляционный пакет загружается во вложенную папку Packages общей папки Сервера администрирования. После загрузки инсталляционный пакет появится в списке инсталляционных пакетов.

В списке инсталляционных пакетов доступных на Сервере администрирования, нажав на имя инсталляционного пакета, вы можете:

- Просмотреть следующие свойства инсталляционного пакета:
  - **Имя**. Название инсталляционного пакета.
  - **Источник**. Имя поставщика приложения.
  - **Приложение**. Название приложения, упакованного в пользовательский инсталляционные пакет.
  - **Версия**. Версия приложения.
  - **Язык**. Язык приложения, упакованного в пользовательский инсталляционный пакет.
  - **Размер (МБ)**. Размер инсталляционного пакета.
  - **Операционная система**. Тип операционной системы, для которой предназначен инсталляционные пакет.
  - **Создано**. Дата создания инсталляционного пакета.
  - **Изменено**. Дата изменения инсталляционного пакета.
  - **Тип**. Тип инсталляционного пакета.
- Изменить имя пакета и параметры командной строки. Эта функция доступна только для пакетов, которые не созданы на основе приложений "Лаборатории Касперского".

Если во время конвертации вы установили рекомендуемые значения параметров для создания пользовательского пакета, могут появиться два дополнительных раздела на вкладке **Параметры** в свойствах пользовательского инсталляционного пакета: **Параметры** и **Последовательность установки**.

Разделе **Параметры** содержит следующие свойства, представленные в таблице:

- **Название**. В этом столбце отображается имя, назначенное параметру установки.
- **Тип**. В этом столбце указан тип параметра установки.
- **Значение**. В этом столбце отображается тип данных, определенный параметром установки (логическое значение, путь к файлу, числовое значение, путь или строковое значение).

Раздел **Последовательность установки** содержит таблицу, в которой описаны следующие свойства обновления, включенного в пользовательский инсталляционный пакет:

- **Название**. 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 (для патчей приложений "Лаборатории Касперского")**. 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**. 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 будет 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.
- **Поставщик**. Отображается имя поставщика обновлений.
- **Семейство приложений**. Отображается имя семейства приложений, к которым относится обновление.
- **Приложение**. Отображается название приложения, которому принадлежит обновление.

- **Язык**. 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.

Распространение инсталляционных пакетов на подчиненные Серверы администрирования

Kaspersky Security Center позволяет вам создавать инсталляционные пакеты для приложений "Лаборатории Касперского" и для приложений сторонних производителей, а также распространять инсталляционные пакеты на клиентские устройства и устанавливать приложения из пакетов. Для оптимизации нагрузки на главном Сервере администрирования вы можете распространять инсталляционные пакеты на подчиненные Серверы администрирования. После этого подчиненные Серверы передают пакеты на клиентские устройства, после чего вы можете выполнять удаленную установку приложений на свои клиентские устройства.

Чтобы распространить инсталляционные пакеты на подчиненные Серверы администрирования:

1. Убедитесь что подчиненные Серверы администрирования подключены к главному Серверу администрирования.
2. в главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.

   Отобразится список задач.
3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
4. На странице **Параметры новой задачи** в раскрывающемся списке **Приложение** выберите **Kaspersky Security Center**. Затем в раскрывающемся списке **Тип задачи** выберите **Распространить инсталляционный пакет** и укажите имя задачи.
5. На странице **Область действия задачи** выберите устройства, которым назначена задача, одним из следующих способов:
   - Если вы хотите сформировать задачу для всех подчиненных Серверов определенной группы администрирования, выберите эту группу и запустите создание групповой задачи для этой группы.
   - Если вы хотите создать задачу для определенных подчиненных Серверов администрирования, выберите эти Серверы и создайте для них задачу.
6. На странице **Распространяемые инсталляционные пакеты** выберите инсталляционные пакеты, которые необходимо скопировать на подчиненные Серверы администрирования.

7. Укажите учетную запись для запуска задачи *Распространение инсталляционного пакета* под этой учетной записью. Вы можете использовать свою учетную запись и оставить включенным параметр **Учетная запись по умолчанию**. Кроме того, можно указать, что задача должна выполняться под другой учетной записью, имеющей необходимые права доступа. Для этого выберите параметр **Задать учетную запись** и введите учетные данные этой учетной записи.

8. На странице **Завершение создания задачи**, можно включить параметр **Открыть окно свойств задачи после ее создания**, чтобы открыть окно свойств задачи и изменить параметры задачи по умолчанию. Также можно настроить параметры задачи позже в любое время.

9. Нажмите на кнопку **Готово**.

   Задача, созданная для распространения инсталляционных пакетов на подчиненные Серверы администрирования, отображается в списке задач.

10. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

После выполнения задачи выбранные инсталляционные пакеты скопированы на указанные подчиненные Серверы администрирования.

Установка приложений с помощью задачи удаленной установки

Kaspersky Security Center позволяет удаленно устанавливать приложения на устройства с помощью задач удаленной установки. Задачи создаются и назначаются устройствам с помощью мастера. Чтобы быстрее и проще назначить задачу устройствам (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**. Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

- **Назначить задачу выборке устройств**. В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать предопределенную выборку 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.

Удаленная установка приложений

Этот раздел содержит информацию о том, как удаленно установить приложение на устройства в группе администрирования, устройства с определенными IP-адресами или набор управляемых устройств.

Чтобы установить приложение на выбранные устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В поле **Тип задачи** выберите **Удаленная установка приложения**.
4. Выберите один из следующих вариантов:

   - **Назначить задачу группе администрирования**

     Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

     Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

     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:

- В поле **Выбор инсталляционного пакета** выберите инсталляционный пакет приложения, которое требуется установить.

- В блоке параметров **Принудительно загрузить инсталляционный пакет** выберите способ доставки на клиентские устройства файлов, необходимых для установки приложения.

  - **С помощью Агента администрирования**

    Если этот параметр включен, доставку инсталляционных пакетов на клиентские устройства выполняет установленный на клиентских устройствах Агент администрирования.

    Если этот параметр выключен, инсталляционные пакеты доставляются с помощью инструментов операционной системы клиентского устройства.

    Рекомендуется включить этот параметр, если задача назначена для устройств с установленными Агентами администрирования.

    По умолчанию параметр включен.

  - **Средствами операционной системы с помощью точек распространения**

    Если флажок установлен, инсталляционные пакеты передаются на клиентские устройства средствами операционной системы через агенты обновлений. Этот вариант можно выбрать, если в сети есть хотя бы один агент обновлений.

    Если установлен флажок **С помощью Агента администрирования**, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

    По умолчанию флажок установлен для задач удаленной установки, созданных на виртуальном Сервере администрирования.

    Единственный способ установить приложение для Windows (включая Агент администрирования для Windows) на устройство, на котором не установлен Агент администрирования, – это использовать точку распространения с операционной системой Windows. Поэтому при установке приложения для Windows:

    - Выберите этот параметр.

    - Убедитесь, что для целевых клиентских устройств назначена точка распространения.

    - Убедитесь, что на точке распространения установлена операционная система Windows.

  - **Средствами операционной системы с помощью Сервера администрирования**

    Если этот параметр включен, доставка файлов на клиентские устройства будет осуществляться средствами операционной системы клиентских устройств с помощью Сервера администрирования. Этот параметр можно включить, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

    По умолчанию параметр включен.

- В поле **Максимальное количество одновременных загрузок** укажите максимально допустимое количество клиентских устройств, на которые Сервер администрирования может одновременно передавать файлы.

- В поле **Максимальное количество попыток установок** укажите максимально допустимое количество запусков приложения установки.

  Если количество попыток, указанное в параметрах задачи, превышено, Kaspersky Security Center больше не запускает приложение установки на устройстве. Чтобы перезапустить задачу *Удаленная установка приложения*, увеличьте значение параметра **Максимальное количество попыток установок** и запустите задачу. Также вы можете создать другую задачу *Удаленная установка приложения*.

- Если вы переносите данные из одного приложения "Лаборатории Касперского" в другую, и ваше текущее приложение защищено паролем, введите пароль в поле **Пароль для удаления приложения "Лаборатории Касперского"**. Обратите внимание, что во время переноса данных ваше текущее приложение "Лаборатории Касперского" будет удалено.

  Поле **Пароль для удаления приложения "Лаборатории Касперского"** доступно, только если вы выбрали параметр **С помощью Агента администрирования** в группе параметров **Принудительно загрузить инсталляционный пакет**.

  Вы можете использовать пароль деинсталляции только для сценария переноса данных Kaspersky Security для Windows Server в Kaspersky Endpoint Security для Windows при установке Kaspersky Endpoint Security для Windows с помощью задачи Удаленная установка приложений. Использование пароля деинсталляции при установке других компонентов может вызвать ошибки установки.

  Для успешного завершения сценария переноса данных убедитесь, что выполнены следующие предварительные условия:

  - Вы используете Агент администрирования Kaspersky Security Center версии 14.2 для Windows или выше.
  - Вы устанавливаете приложение на устройства под управлением Windows.

- Настройте дополнительный параметр:

  - **Не устанавливать приложение, если оно уже установлено**

    Если этот параметр включен, выбранное приложение не устанавливается заново, если оно уже установлено на клиентском устройстве.

    Если этот параметр выключен, приложение будет установлено в любом случае.

    По умолчанию параметр включен.

  - **Предварительно проверять тип операционной системы перед загрузкой**

    Перед передачей файлов на клиентские устройства Kaspersky Security Center проверяет, применимы ли параметры утилиты установки к операционной системе клиентского устройства. Если параметры не применимы, Kaspersky Security Center не передает файлы и не пытается установить приложение. Например, чтобы установить некоторые приложения на устройства группы администрирования, в которую входят устройства с различными операционными системами, вы можете назначить задачу установки группе администрирования, а затем включить этот параметр, чтобы пропускать устройства с операционной системой, отличной от требуемой.

    При удаленной установке Агента администрирования на нераспределенные устройства Kaspersky Security Center или точка распространения автоматически определяет тип операционной системы устройства независимо от параметра **Предварительно проверять тип операционной системы перед загрузкой**.

- **Назначить установку инсталляционного пакета в групповых политиках Active Directory**

  Если этот параметр включен, инсталляционный пакет будет устанавливаться с помощью групповых политик Active Directory.

  Параметр доступен, если выбран инсталляционный пакет Агента администрирования.

  По умолчанию параметр выключен.

- **Предлагать пользователю закрыть работающие приложения**

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.

- Выберите, на какие устройства вы хотите установить приложение:

  - **Устанавливать на все устройства**

    Приложение устанавливается даже на устройства, управляемые другими Серверами администрирования.

    По умолчанию этот вариант выбран. Не нужно изменять этот параметр, если в вашей сети есть только один Сервер администрирования.

  - **Устанавливать на устройства, управляемые только этим Сервером администрирования**

    Приложение устанавливается только на устройства, которые управляются данным Сервером администрирования. Выберите этот параметр, если в вашей сети установлено больше одного Сервера администрирования и вы хотите избежать конфликтов между ними.

- Укажите, следует ли перемещать устройства в группу администрирования после установки:

  - **Не перемещать устройства**

    Устройства остаются в тех группах, к которым они принадлежат. Устройства, не принадлежащие ни к одной из групп, остаются нераспределенными.

  - **Переместить нераспределенные устройства в выбранную группу (можно выбрать только одну группу)**

    Устройства перемещаются в выбранную вами группу администрирования.

  Обратите внимание, что по умолчанию выбран вариант **Не перемещать устройства**. По соображениям безопасности вы можете предпочесть перемещение устройств вручную.

7. На этом шаге мастера укажите, требуется ли перезагрузка устройства при установке приложений:

- **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.

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 учетная запись**. Если выбран этот вариант, укажите учетную запись пользователя, от имени которой будет запускаться установщик приложения. Нажмите на кнопку **Добавить**, выберите **Локальная учетная запись** и укажите данные учетной записи пользователя.

       Вы можете указать несколько учетных записей, если ни одна из них не обладает необходимыми правами на всех устройствах, для которых назначена задача. В этом случае для запуска задачи используются последовательно, сверху вниз, все добавленные учетные записи.

     - **SSH сертификат**. Если вы хотите установить 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 поддерживает формат закрытых ключей PEM, а утилита ssh-keygen по умолчанию генерирует SSH-ключи в формате OPENSSH. Формат OPENSSH не поддерживается Kaspersky Security Center. Чтобы создать закрытый ключ в поддерживаемом формате PEM, добавьте параметр -m PEM в команду ssh-keygen. Например:

       ```
       ssh-keygen -m PEM -t rsa -b 4096 -C "<электронная почта пользователя>"
       ```

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 приложения с помощью групповых политик Active Directory

Kaspersky Security Center позволяет устанавливать приложения "Лаборатории Касперского" на управляемые устройства с помощью групповых политик Active Directory.

Установка приложений с помощью групповых политик Active Directory возможна только из инсталляционных пакетов, в состав которых входит Агент администрирования.

Чтобы установить приложение с помощью групповых политик Active Directory:

1. Запустите мастер развертывания защиты. Следуйте далее указаниям мастера.
2. На странице **Параметры задачи удаленной установки** мастера развертывания защиты выберите параметр **Назначить установку инсталляционного пакета в групповых политиках Active Directory**.
3. На странице **Выбор учетных записей для доступа к устройствам** выберите параметр **Учетная запись требуется (Агент администрирования не используется)**.
4. Добавьте учетную запись с правами администратора на устройство, на котором установлен Kaspersky Security Center, или учетную запись, входящую в доменную группу Владельцы-создатели групповой политики.
5. Предоставьте разрешения выбранной учетной записи:
   a. Перейдите в **Панель управления** → **Администрирование** и откройте **Управление групповой политикой**.
   b. Нажмите на узел с нужным доменом.
   c. Нажмите на раздел **Делегирование**.
   d. В раскрывающемся списке **Права доступа** выберите **Связанные объекты GPO**.
   e. Нажмите на кнопку **Добавить**.
   f. В открывшемся окне **Выбор пользователя, компьютера или группы** выберите необходимую учетную запись.
   g. Нажмите на кнопку **OK** чтобы закрыть окно **Выбор пользователя, компьютера или группы**.
   h. В списке **Группы и пользователи** выберите только что добавленную учетную запись и нажмите на **Дополнительно** → **Дополнительно**.
   i. В списке **записей разрешений** дважды нажмите на только что добавленную учетную запись.
   j. Предоставьте следующие разрешения:
      - **создание объектов группы;**
      - **удаление объектов группы;**

- **создание объектов контейнера групповой политики;**
- **удаление объектов контейнера групповой политики.**

k. Нажмите на кнопку **OK**, чтобы сохранить изменения.

6. Задайте другие параметры, следуя инструкциям мастера.
7. Запустите созданную задачу удаленной установки вручную или дождитесь ее запуска по расписанию.

В результате будет запущен следующий механизм удаленной установки:

1. После запуска задачи в каждом домене, которому принадлежат клиентские устройства из набора, будут созданы следующие объекты:
   - Объект групповой политики (Group policy object, GPO) с именем **Kaspersky_AK{GUID}**.
   - Группа безопасности содержит клиентские устройства, на которые распространяется задача. Эта группа безопасности содержит клиентские устройства, на которые распространяется задача. Состав группы безопасности определяет область объект групповой политики (GPO).
2. Kaspersky Security Center устанавливает выбранные приложения "Лаборатории Касперского" на клиентские устройства непосредственно из сетевой папки общего доступа приложения KLSHARE. При этом в папке установки Kaspersky Security Center будет создана вложенная вспомогательная папка, содержащая файл с расширением msi для устанавливаемого приложения.
3. При добавлении новых устройств в область действия задачи они будут добавлены в группу безопасности после следующего запуска задачи. Если в расписании задачи выбран флажок **Запускать пропущенные задачи**, устройства будут добавлены в группу безопасности сразу.
4. При удалении устройств из области действия задачи их удаление из группы безопасности произойдет при следующем запуске задачи.
5. При удалении задачи из Active Directory будут удалены объект групповой политики (GPO), ссылка на объект групповой политики (GPO) и группа безопасности, связанная с задачей.

Если вы хотите использовать другую схему установки через Active Directory, вы можете настроить параметры установки вручную. Это может потребоваться, например, в следующих случаях:

- при отсутствии у администратора антивирусной защиты прав на внесение изменений в Active Directory некоторых доменов;
- при необходимости размещения исходного дистрибутива на отдельном сетевом ресурсе;
- для привязки групповой политики к конкретным подразделениям Active Directory.

Доступны следующие варианты использования другой схемы установки через Active Directory:

- Если установку требуется осуществлять непосредственно из папки общего доступа Kaspersky Security Center, в свойствах групповой политики Active Directory следует указать файл с расширением msi, расположенный во вложенной папке exec в папке инсталляционного пакета нужного приложения.
- Если инсталляционный пакет нужно разместить на другом сетевом ресурсе, следует скопировать в него все содержимое папки exec, так как помимо файла с расширением msi в ней содержатся конфигурационные файлы, сформированные при создании инсталляционного пакета. Чтобы лицензионный ключ был установлен вместе с приложением, в эту папку следует также скопировать файл ключа.

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.

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 **Активы (Устройства)** → **Задачи**.

2. Нажмите на имя задачи удаленной установки, для которой вы хотите указать параметры, специфичные для Unix.

   Откроется окно свойств задачи.

3. Перейдите в 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 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 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 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.

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 **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В раскрывающемся списке **Приложение** выберите приложение, для которого вы хотите создать задачу.

   Приложения "Лаборатории Касперского" отображаются в списке, если вы ранее добавили веб-плагины управления этих приложений.
4. В списке **Тип задачи** выберите задачу **Активация приложения**.
5. В поле **Название задачи** укажите название новой задачи.

   Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
6. Выберите устройства, которым будет назначена задача.
7. В окне **Приложения** выполните следующее:

   - Установите флажки рядом с названиями приложений, для которых вы хотите создать задачу.
   - Выберите параметр **Запустить приложение** или **Остановить приложение**.

8. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на шаге **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

9. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.

10. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

11. В окне свойств задачи укажите общие параметры задачи в соответствии с вашими требованиями и сохраните параметры.

Задача создана и настроена.

Если вы хотите запустить задачу, выберите задачу в списке задач и нажмите на кнопку **Запустить**.

Управление мобильными устройствами

Управление защитой мобильными устройствами через Kaspersky Security Center 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 Endpoint Security for Android, установленное на устройствах. Это мобильное приложение обеспечивает защиту мобильных устройств от веб-угроз, вирусов и других приложений, которые представляют собой угрозы. Для централизованного управления через Kaspersky Security Center Web Console необходимо установить следующие веб-плагины управления на устройство, на котором установлено приложение Kaspersky Security Center Web Console:

- Плагин Kaspersky Security для мобильных устройств
- Плагин Kaspersky Endpoint Security for Android

Информацию о развертывании защиты и управлении мобильными устройствами см. в справке Kaspersky Security для мобильных устройств.

Изменение параметров Управления мобильными устройствами в Kaspersky Security Center Web Console

Чтобы изменить параметры Управления мобильными устройствами:

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 **Дополнительные порты**.

3. Измените требуемые параметры:

- **Открыть порт для мобильных устройств**

  Если этот переключатель включен, на Сервере администрирования будет открыт порт для мобильных устройств.

  Использование порта для мобильных устройств возможно только в случае, если установлен компонент Управление мобильными устройствами.

  Если переключатель выключен, порт для мобильных устройств на Сервере администрирования не используется.

  По умолчанию переключатель выключен.

- **Порт для синхронизации мобильных устройств**

  Номер порта, по которому осуществляется подключение мобильных устройств к Серверу администрирования. По умолчанию установлен порт 13292.

  Используется десятичная форма записи.

- **Порт для активации мобильных устройств**

  Порт подключения Kaspersky Endpoint Security для Android к серверам активации "Лаборатории Касперского".

  По умолчанию установлен порт 17100.

4. Нажмите на кнопку **Сохранить**.

Мобильные устройства могут подключаться к Серверу администрирования.

Замещение приложений безопасности сторонних производителей

Для установки приложения безопасности "Лаборатории Касперского" средствами Kaspersky Security Center может потребоваться удалить приложение стороннего производителя, несовместимое с устанавливаемым приложением. Kaspersky Security Center предоставляет несколько способов удаления приложений сторонних производителей.

Удаление несовместимых приложений с помощью приложения установки

Этот параметр доступен только в Консоли администрирования на основе консоли управления Microsoft Management Console.

Метод удаления несовместимых приложений поддерживается различными типами установки. Перед установкой приложения безопасности несовместимые с ним приложения удаляются автоматически, если в окне свойств инсталляционного пакета приложений безопасности (раздел **Несовместимые приложения**) выбран параметр **Удалять несовместимые приложения автоматически**.

Удаление несовместимых приложений при настройке удаленной установки приложения

Вы можете включить параметр **Удалять несовместимые приложения автоматически** во время настройки удаленной установки приложения безопасности. В Консоли администрирования на основе консоли Microsoft Management Console (MMC) этот параметр доступен в мастере удаленной установки. В приложении Kaspersky Security Center Web Console этот параметр можно найти в мастере развертывания защиты. Если этот параметр включен, Kaspersky Security Center удаляет несовместимые приложения перед установкой приложения безопасности на управляемое устройство.

Инструкции:

- Консоль администрирования: Удаление несовместимых приложений с помощью мастера удаленной установки.
- Kaspersky Security Center Web Console: Удаление несовместимых приложений перед установкой.

Удаление несовместимых приложений с помощью отдельной задачи

Для удаления несовместимых приложений используется задача **Удаленная деинсталляция приложений**. 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.

Инструкции для Консоли администрирования: Создание задачи.

Обнаружение устройств в сети

В этом разделе описаны поиск устройств и опрос сети.

Kaspersky Security Center позволяет искать устройства на основании заданных критериев. Вы можете сохранить результаты поиска в текстовый файл.

Функция поиска позволяет находить следующие устройства:

- управляемые устройства в группах администрирования Сервера администрирования Kaspersky Security Center и его подчиненных Серверов;
- нераспределенные устройства под управлением Сервера администрирования Kaspersky Security Center и его подчиненных Серверов.

Сценарий: обнаружение сетевых устройств

Вам нужно выполнить поиск устройств перед установкой приложений безопасности. Сервер администрирования получает информацию об обнаруженных устройствах и позволяет управлять устройствами с помощью политик. Регулярные опросы сети необходимы для обновления списка устройств, доступных в сети.

Прежде чем начать опрос сети, убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

Обнаружение сетевых устройств содержит следующие этапы:

1. **Обнаружение устройств**

   Мастер первоначальной настройки выполняет начальное обнаружение устройств и помогает найти сетевые устройства, такие как компьютеры, планшеты и мобильные телефоны. Вы можете также запустить обнаружение устройств вручную.

2. **Настройка расписания опросов**

   Определите, какой тип опроса вы хотите регулярно использовать. Включите требуемые типы и настройте расписание опроса. Также см. рекомендации по частоте опроса сети.

3. **Задание правил для добавления обнаруженных устройств в группы администрирования (если требуется)**

   Новые устройства появляются в сети в результате их обнаружения при опросах сети. Они автоматически попадают в группу **Нераспределенные устройства**. Можно настроить правила перемещения устройств, в соответствии с которыми устройства будут распределены в группу **Управляемые устройства**. Можно также настроить правила хранения.

   Если вы пропустили шаг 3, список новых обнаруженных устройств располагается в группе **Нераспределенные устройства**. Вы можете переместить эти устройства в группу **Управляемые устройства** вручную. Если вы вручную переместили устройства в группу **Управляемые устройства**, вы можете проанализировать информацию о каждом из устройств и решить, требуется ли переместить его в группу администрирования и в какую.

Результаты

Завершение сценария дает следующее:

- Сервер администрирования Kaspersky Security Center обнаруживает устройства в сети и предоставляет информацию о них.
- Настроены будущие опросы сети и расписание их запуска.
- Новые обнаруженные устройства распределены в соответствии с заданными правилами. Если правила не заданы, устройства остаются в группе **Нераспределенные устройства**.

Обнаружение устройств

В этом разделе описаны типы обнаружения устройств, доступные в Kaspersky Security Center, а также приведена информация об использовании каждого из них.

Во время регулярных опросов сети Сервер администрирования получает информацию о структуре сети и устройствах в сети. Данные записываются в базу данных Сервера администрирования. Сервер администрирования может проводить следующие типы опросов сети:

- **Опрос сети Windows**. Сервер администрирования может проводить два типа опросов сети Windows: быстрый и полный. При быстром опросе Сервер администрирования получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети. При полном опросе с каждого клиентского устройства запрашивается более подробная информация, например, имя операционной системы, IP-адрес, DNS-имя и NetBIOS-имя. По умолчанию включены быстрый и полный опрос. При опросе сети Windows может не удаться обнаружить устройства, например, если роутером или сетевым экраном закрыты порты UDP 137, UDP 138, TCP 139.

- **Опрос контроллеров домена**. Сервер администрирования или точка распространения получает информацию о структуре домена и DNS-именах устройств, входящих в домен. По умолчанию этот тип опроса включен. Рекомендуется использовать опрос контроллеров домена, если все сетевые устройства являются членами домена. Если некоторые из сетевых устройств не включены в домен, эти устройства не могут быть обнаружены с помощью опроса контроллеров домена.

- **Опрос IP-диапазонов**. Сервер администрирования опрашивает указанные IP-диапазоны с помощью ICMP-пакетов или NBNS-протоколов и получает полную информацию об устройствах, входящих в IP-диапазоны. По умолчанию этот тип опроса выключен. Не рекомендуется использовать этот тип опроса, если вы используете опрос сети Windows и/или опрос Active Directory.

- **Опрос Zeroconf**. Точка распространения выполняет опрос IPv6-сети, используя сеть с нулевой конфигурацией (далее также *Zeroconf*). По умолчанию этот тип опроса выключен. Вы можете использовать опрос Zeroconf, если точка распространения работает под управлением Linux.

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**.

Можно изменить параметры обнаружения устройств для каждого типа. Например, может потребоваться изменить расписание опроса или указать, нужно опрашивать весь лес доменов или только определенный домен.

Прежде чем начать опрос сети, убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

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, UDP 445, TCP 445;
- SMB-протокол включен;
- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на Сервере администрирования;
- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на клиентском устройстве:
  - наличие хотя бы одного устройства, если количество сетевых устройств не превышает 32;
  - наличие как минимум одного устройства на каждые 32 сетевых устройства.

Полный опрос сети может быть запущен, только если быстрый опрос был запущен как минимум один раз.

Просмотр и изменение параметров опроса сети Windows

Чтобы изменить параметры опроса сети Windows:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Windows-домены**.
2. Нажмите на кнопку **Свойства**.

   Откроется окно свойств Windows-домена.
3. Включите или выключите опрос Windows сети, используя переключатель **Включить опрос сети Windows**.
4. Настройте расписание опроса. По умолчанию быстрый опрос запускается каждые 15 минут, а полный опрос запускается каждые 60 минут.

Варианты расписания опроса:

- **Каждые N дней**

  Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

  По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

- **Каждые N минут**

  Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

- **По дням недели**

  Опрос выполняется регулярно, в указанные дни недели, в указанное время.

- **Ежемесячно, в указанные дни выбранных недель**

  Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

- **Запускать пропущенные задачи**

  Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

  Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

  Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

  По умолчанию параметр выключен.

5. Сохраните параметры опроса сети Windows.

Параметры сохранены и применены ко всем Windows-доменам и рабочим группам.

Запуск опроса вручную

Чтобы запустить проверку немедленно,

нажмите **Начать быстрый опрос** или **Начать полный опрос**.

Когда опрос завершен, вы можете просмотреть список обнаруженных устройств на странице **Windows-домены**, установив флажок рядом с именем домена, а затем нажать на кнопку **Устройства**.

Опрос IP-диапазонов

Исходно Kaspersky Security Center получает IP-диапазоны для опроса из сетевых параметров устройства, на которое он установлен. Если адрес устройства 192.168.0.1, а маска подсети – 255.255.255.0, Kaspersky Security Center автоматически включит сеть 192.168.0.0/24 в список адресов для опроса. Kaspersky Security Center выполнит опрос всех адресов от 192.168.0.1 до 192.168.0.254.

Для всех устройств с операционной системой Linux в контроллере домена Microsoft Active Directory или Samba укажите `netbios name` и параметры `workgroup` в файле `/etc/samba/smb.conf`. Иначе результаты опроса могут содержать дублирующиеся устройства.

Kaspersky Security Center может опрашивать диапазоны IP-адресов путем обратного поиска DNS или по NBNS-протоколу:

- **обратный поиск DNS;**

  Kaspersky Security Center 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. 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. 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 сервисов. Из-за этих причин опрос IP-подсети по умолчанию отключен.

- **NBNS-протокол.**

  Если обратное разрешение имен в вашей сети по каким-либо причинам невозможно, Kaspersky Security Center использует NBNS-протокол для опроса IP-диапазонов. Если запрос к IP-адресу возвращает NetBIOS-имя, информация об этом устройстве добавляется в базу данных Kaspersky Security Center.

Прежде чем начать опрос сети, убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

Просмотр и изменение параметров опроса IP-диапазонов

Чтобы просмотреть и изменить параметры опроса IP-диапазонов:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **IP-диапазоны**.

2. Нажмите на кнопку **Свойства**.

   Откроется окно свойств опроса IP-диапазонов.

3. Включите или выключите опрос IP-диапазонов, используя переключатель **Разрешить опрос**.

4. Настройте расписание опроса. По умолчанию опрос IP-диапазонов запускается каждые 420 минут (семь часов).

   При указании интервала опроса убедитесь, что его значение не превышает значения параметра время действия IP-адреса. Если IP-адрес не подтвержден при опросе в течение времени действия IP-адреса, он автоматически удаляется из результатов опроса. По умолчанию срок существования запросов составляет 24 часа, поскольку динамические IP-адреса, назначенные по протоколу DHCP (Dynamic Host Configuration Protocol – протокол динамической конфигурации сетевого узла), меняются каждые 24 часа.

Варианты расписания опроса:

- **Каждые N дней**

  Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

  По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

- **Каждые N минут**

  Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

- **По дням недели**

  Опрос выполняется регулярно, в указанные дни недели, в указанное время.

- **Ежемесячно, в указанные дни выбранных недель**

  Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

- **Запускать пропущенные задачи**

  Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

  Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

  Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

  По умолчанию параметр выключен.

5. Нажмите на кнопку **Сохранить**.

Параметры будут сохранены и применены ко всем IP-диапазонам.

Запуск опроса вручную

Чтобы запустить проверку немедленно,

нажмите на кнопку **Начать опрос**.

Добавление и изменение IP-диапазона

Исходно Kaspersky Security Center получает IP-диапазоны для опроса из сетевых параметров устройства, на которое он установлен. Если адрес устройства 192.168.0.1, а маска подсети – 255.255.255.0, Kaspersky Security Center автоматически включит сеть 192.168.0.0/24 в список адресов для опроса. Kaspersky Security Center выполнит опрос всех адресов от 192.168.0.1 до 192.168.0.254. Вы можете изменять автоматически определенные IP-диапазоны или добавлять собственные IP-диапазоны.

Вы можете создать диапазон только для IPv4-адресов. Если вы включите опрос Zeroconf, Kaspersky Security Center будет опрашивать всю сеть.

Чтобы добавить новый IP-диапазон:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **IP-диапазоны**.

2. Чтобы добавить IP-диапазон, нажмите на кнопку **Добавить**.

3. В открывшемся окне настройте следующие параметры:

   - **Имя IP-диапазона**

     Имя IP-диапазона. Вы можете указать IP-диапазон по имени, например, 192.168.0.0/24.

   - **IP-интервал или адрес и маска подсети**

     Задайте IP-диапазон, указав либо начальный и конечный IP-адреса, либо адрес подсети и маску подсети. Можно также выбрать один из существующих диапазонов IP-адресов, нажав на кнопку **Обзор**.

   - **Время действия IP-адреса (ч)**

     При задании этого параметра убедитесь, что он превышает значение интервала опроса, заданного в расписании опроса. Если IP-адрес не подтвержден при опросе в течение времени действия IP-адреса, он автоматически удаляется из результатов опроса. По умолчанию срок существования запросов составляет 24 часа, поскольку динамические IP-адреса, назначенные по протоколу DHCP (Dynamic Host Configuration Protocol – протокол динамической конфигурации сетевого узла), меняются каждые 24 часа.

4. Выберите **Разрешить опрос IP-диапазона**, если вы хотите опрашивать подсеть или интервал, который вы указали. В противном случае подсеть или интервал, которые вы добавили, не будут опрошены.

5. Нажмите на кнопку **Сохранить**.

IP-диапазон добавлен в список IP-диапазонов.

Вы можете запустить опрос для каждого IP-диапазона в отдельности, используя кнопку **Начать опрос**. После завершения опроса вы можете просмотреть список обнаруженных устройств, нажав на кнопку **Устройства**. По умолчанию срок действия результатов опроса составляет 24 часа, он равен времени действия IP-адреса.

Чтобы добавить подсеть в существующий IP-диапазон:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **IP-диапазоны**.

2. Нажмите на имя IP-диапазона, в который вы хотите добавить подсеть.

3. В появившемся окне нажмите на кнопку **Добавить**.

4. Укажите подсеть либо с помощью ее адреса и маски, либо задав первый и последний IP-адреса в IP-диапазоне. Или добавить существующую подсеть, нажав на кнопку **Обзор**.

5. Нажмите на кнопку **Сохранить**.

   Подсеть добавлена в IP-диапазон.

6. Нажмите на кнопку **Сохранить**.

Параметры IP-диапазона сохранены.

Вы можете добавить столько подсетей, сколько необходимо. Именованные IP-диапазоны не должны пересекаться, но на неименованные подсети внутри IP-диапазонов это ограничение не распространяется. Вы можете включить или отключить опрос независимо для каждого IP-диапазона.

Опрос Zeroconf

Этот тип опроса поддерживается только для точек распространения с операционными системами Linux.

Точка распространения может опрашивать сети, в которых есть устройства с IPv6-адресами. В этом случае IP-диапазоны не указываются, и точка распространения опрашивает всю сеть, используя сеть с нулевой конфигурацией (далее также *Zeroconf*). Чтобы начать использовать Zeroconf, вам нужно установить утилиту avahi-browse на точке распространения.

Чтобы включить опрос IPv6-сети:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **IP-диапазоны**.

2. Нажмите на кнопку **Свойства**.

3. В открывшемся окне нажмите на кнопку **Использовать Zeroconf для опроса IPv6-сетей**.

После этого точка распространения начинает опрашивать вашу сеть. В этом случае указанные IP-диапазоны игнорируются.

Опрос контроллеров домена

Kaspersky Security Center поддерживает опрос контроллеров домена Microsoft Active Directory и контроллеров домена Samba.

Kaspersky Security Center позволяет 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 контроллера домена Сервер администрирования или точка распространения получают информацию о структуре домена, учетных записях пользователей, группах безопасности и о DNS-именах устройств, входящих в домен.

Рекомендуется использовать опрос контроллеров домена, если все сетевые устройства являются членами домена. Если некоторые из сетевых устройств не включены в домен, эти устройства не могут быть обнаружены с помощью опроса контроллеров домена.

Предварительные требования

Перед опросом контроллера домена убедитесь, что вы разрешаете подключения к контроллеру домена через сетевой экран или прокси-сервер. Также убедитесь, что на контроллере домена включены следующие протоколы:

- Lightweight Directory Access Protocol (LDAP).
- Simple Authentication and Security Layer (SASL).

  Этот протокол используется, если соединение с контроллером домена установлено с использованием SASL-аутентификации. Сервер администрирования и точки распространения поддерживают только механизм DIGEST-MD5.
- Lightweight Directory Access Protocol через Secure Sockets Layer (LDAPS)

  Этот протокол используется, если вам нужно подключиться к контроллеру домена по зашифрованному подключению.

Необходимо убедиться, что на устройстве контроллеров домена доступны следующие порты:

- 389 для LDAP-протокола и Simple Authentication (включая SASL).
- 636 для LDAPS-протокола.

Для всех устройств с операционной системой Linux в контроллере домена Microsoft Active Directory или Samba вам нужно указать `netbios name` и параметры `workgroup` в файле `/etc/samba/smb.conf`. Иначе результаты опроса могут содержать дублирующиеся устройства.

> Если домен Microsoft Active Directory содержит несколько контроллеров домена, выбор конкретного контроллера во время опроса домена не поддерживается. Соединение устанавливается с первым обнаруженным контроллером домена. Для обеспечения корректной аутентификации в домене Microsoft Active Directory поле альтернативного имени субъекта (SAN) сертификата должно включать все адреса контроллеров домена, входящих в этот домен, а также NetBIOS-имя домена Microsoft Active Directory.

Опрос контроллеров домена с помощью Сервера администрирования

Вы можете использовать Сервер администрирования для опроса только контроллера домена Microsoft Active Directory.

Чтобы опросить контроллеры домена с помощью Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Контроллеры доменов**.
2. Нажмите на кнопку **Параметры опроса**.

   Откроется окно **Параметры опроса контроллеров домена**.
3. Выберите параметр **Включить опрос контроллеров домена**.

4. В разделе **Дополнительные параметры** укажите область опроса:

   - **Опросить текущий домен**

     Выберите этот параметр, чтобы опросить домен, которому принадлежит Kaspersky Security Center.

   - **Опросить весь лес доменов**

     Выберите этот параметр, чтобы опросить лес доменов, к которому принадлежит Kaspersky Security Center.

   - **Опросить указанные домены**

     Выберите этот параметр, чтобы опросить домен с указанным адресом и учетными данными пользователя.

5. При необходимости настройте расписание опроса. По умолчанию период опроса составляет один час. Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

   Доступны следующие варианты расписания опроса сети:

   - **Каждые N дней**

     Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

     По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

   - **Каждые N минут**

     Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

   - **По дням недели**

     Опрос выполняется регулярно, в указанные дни недели, в указанное время.

   - **Ежемесячно, в указанные дни выбранных недель**

     Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

   - **Запускать пропущенные задачи**

     Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

     Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

     Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

     По умолчанию параметр выключен.

   Если вы измените учетные записи пользователей в группе безопасности домена, эти изменения отобразятся в Kaspersky Security Center через час после опроса контроллеров домена.

6. Нажмите на кнопку **Сохранить**, чтобы применить изменения.

7. Если требуется запустить опрос сети немедленно, нажмите на кнопку **Начать опрос**.

Опрос контроллеров домена с помощью точки распространения

Вы также можете опросить контроллер домена Microsoft Active Directory и контроллер домена Samba с помощью точки распространения. Управляемое устройство с операционной системой Windows или Linux может выступать в роли точки распространения.

Для точки распространения с операционной системой Linux поддерживается опрос контроллеров домена Microsoft Active Directory и контроллеров домена Samba.
Для точки распространения с операционной системой Windows поддерживается только опрос контроллеров домена Microsoft Active Directory.
Опрос с помощью точки распространения с операционной системой Mac не поддерживается.

Чтобы настроить опрос контроллеров домена с помощью точки распространения:

1. Откройте свойства точки распространения.
2. Выберите раздел **Опрос контроллеров домена**.
3. Выберите параметр **Включить опрос контроллеров домена**.
4. Выберите контроллеры домена, которые вы хотите опросить.

   Если вы используете точку распространения с операционной системой Linux, в разделе **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**
5. Нажмите на кнопку **Настроить расписание опроса**, чтобы указать параметры расписания опроса при необходимости.

   Опрос запускается в соответствие с расписанием. Запуск опроса вручную недоступен.

После завершения опроса в разделе **Контроллеры доменов** отобразится структура домена.

Если вы настроили и включили правила перемещения устройств, новые обнаруженные устройства будут автоматически перемещаться в группу **Управляемые устройства**. Если правила перемещения устройств не включены, новые обнаруженные устройства будут автоматически перемещаться в группу **Нераспределенные устройства**.

Обнаруженные учетные записи пользователей могут быть использованы для доменной аутентификации в Kaspersky Security Center Web Console.

Аутентификация и подключение к контроллеру домена

Аутентификация и подключение к контроллеру домена при опросе домена

При опросе контроллера домена точкой распространения с операционной системой Linux, точка распространения определяет протокол соединения для установления начального соединения с контроллером домена. Этот протокол используется для всех будущих подключений к контроллеру домена. При первоначальном подключении к контроллеру домена вы можете изменить параметры подключения с помощью флагов Агента администрирования `KLNAG_LDAP_TLS_REQCERT` и `KLNAG_LDAP_SSL_CACERT`. Вы можете настроить флаги Агента администрирования с помощью команды klscflag, как описано в этой статье.

Первоначальное подключение к контроллеру домена происходит следующим образом:

1. Точка распространения с операционной системой Linux пытается подключиться к контроллеру домена через LDAPS.

   По умолчанию проверка сертификата не требуется. Для флага `KLNAG_LDAP_TLS_REQCERT` установите значение 1, чтобы принудительно выполнить проверку сертификата.

   Возможные значения флага `KLNAG_LDAP_TLS_REQCERT`:

   - `0` – сертификат запрошен, но если он не предоставлен или проверка сертификата завершилась неудачно, соединение TLS по-прежнему считается успешно созданным (значение по умолчанию).
   - `1` – требуется строгая проверка сертификата LDAP-сервера.

   По умолчанию, если флаг `KLNAG_LDAP_SSL_CACERT` не задан, для доступа к цепочке сертификатов используется зависящий от операционной системы путь к центру сертификации (CA). Используйте флаг `KLNAG_LDAP_SSL_CACERT`, чтобы указать другой путь.

2. В случае сбоя LDAPS-соединения точка распространения с операционной системой Linux пытается подключиться к контроллеру домена по незашифрованному TCP-соединению с помощью SASL (DIGEST-MD5).

Настройка флагов

Вы можете использовать утилиту klscflag для настройки флагов.

На точке распространения с операционной системой Linux запустите командную строку и измените текущую директорию на директорию с утилитой klscflag. По умолчанию на точке распространения с операционной системой Linux утилита klscflag находится в папке /opt/kaspersky/ksc64/sbin.

Например, следующая команда принудительно проверяет сертификат:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

Настройка контроллеров домена Samba

Kaspersky Security Center поддерживает контроллеры домена Linux, работающие только на Samba 4.

Контроллер домена Samba поддерживает те же расширения схемы, что и контроллер домена Microsoft Active Directory. Вы можете включить полную совместимость контроллера домена Samba с контроллером домена Microsoft Active Directory, используя расширение схемы Samba 4. Это необязательное действие.

Рекомендуется включить полную совместимость контроллера домена Samba с контроллером домена Microsoft Active Directory. Это обеспечит корректное взаимодействие Kaspersky Security Center и контроллером домена Samba.

Чтобы включить полную совместимость контроллера домена Samba с контроллером домена Microsoft Active Directory:

1. Выполните следующую команду, чтобы использовать расширение схемы RFC2307:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Включите обновление схемы на контроллере домена Samba. Для этого добавьте следующую строку в файл `/etc/samba/smb.conf`:

   ```
   dsdb:schema update allowed = true
   ```

   Если обновление схемы завершается с ошибкой, необходимо выполнить полное восстановление контроллера домена, который выполняет роль схемы master.

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.

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 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 **ОК**.

   Откроется окно свойств устройства на разделе **Общие**.

5. В разделе **Общие** заполните поля ввода данными об устройстве. В разделе **Общие** доступны следующие параметры:

   - **Корпоративное устройство**. Установите флажок, если вы хотите присвоить устройству признак *Корпоративное*. По этому признаку можно выполнять поиск устройств в папке **Оборудование**.
   - **Списано**. Установите флажок, если вы не хотите, чтобы устройство отображалось в списке устройств в папке **Оборудование**.

6. Нажмите на кнопку **Применить**.

Новое устройство отобразится в рабочей области страницы **Оборудование**.

Настройка критериев определения корпоративных устройств

Чтобы настроить критерии определения корпоративных устройств:

1. В главном окне приложения перейдите в раздел **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 **ОК**.

Критерии обнаружения корпоративных устройств настроены.

Приложения "Лаборатории Касперского": лицензирование и активация

В этом разделе описаны возможности Kaspersky Security Center по работе с лицензионными ключами управляемых приложений "Лаборатории Касперского".

Kaspersky Security Center позволяет централизованно распространять лицензионные ключи приложений "Лаборатории Касперского" на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.

При добавлении лицензионного ключа с помощью Kaspersky Security Center свойства лицензионного ключа сохраняются на Сервере администрирования. На основании этой информации приложение формирует отчет об использовании лицензионных ключей и уведомляет администратора об истечении сроков действия лицензий и о превышении лицензионных ограничений, заложенных в свойствах лицензионных ключей. Вы можете настраивать параметры оповещений об использовании лицензионных ключей в составе параметров Сервера администрирования.

Лицензирование управляемых приложений

Приложения "Лаборатории Касперского" установленные на управляемых устройствах, должны быть активированы путем применения файла ключа или кода активации к каждому из приложений. Файл ключа или код активации может быть распространен следующими способами:

- с помощью автоматического распространения;
- с помощью инсталляционного пакета управляемого приложения;
- с помощью задачи *Добавление лицензионного ключа* управляемого приложения;
- активация управляемого приложения вручную.

Вы можете добавить активный или резервный лицензионный ключ любым из перечисленных выше способов. Приложение "Лаборатории Касперского" использует активный в данный момент ключ и сохраняет резервный ключ, который будет применяться после истечения срока действия активного ключа. Приложение, для которого вы добавляете лицензионный ключ, определяет, является ли ключ активным или резервным. Определение ключа не зависит от способа, который вы используете для добавления лицензионного ключа.

Автоматическое распространение

Если вы используете разные управляемые приложения и вам важно распространить определенный файл ключа или код активации на устройства, используйте другие способы распространения кода активации или файла ключа.

Kaspersky Security Center позволяет автоматически распространять имеющиеся лицензионные ключи на устройства. Например, в хранилище Сервера администрирования находится три лицензионных ключа. Для всех лицензионных ключей установлен флажок **Автоматически распространять лицензионный ключ на управляемые устройства**. На устройствах организации установлено приложение безопасности "Лаборатории Касперского", например, Kaspersky Endpoint Security для Windows. Обнаружено новое устройство, на которое необходимо распространить лицензионный ключ. Приложение определяет, что для этого устройства подходит, например, два лицензионных ключа из хранилища, лицензионный ключ *Ключ_1* и лицензионный ключ *Ключ_2*. На устройство распространяется один из подходящих лицензионных ключей. В этом случае невозможно предсказать, какой из этих двух лицензионных ключей будет распространен на данное устройство, так как автоматическое распространение лицензионных ключей не предполагает вмешательства администратора.

При распространении лицензионного ключа на устройства происходит подсчет устройств для данного лицензионного ключа. Вам необходимо удостовериться, что количество устройств, на которые распространяется лицензионный ключ, не превышает лицензионное ограничение. В случае если количество устройств превышает лицензионное ограничение, таким устройствам будет присвоен статус *Критический*.

Перед распространением файл ключа или код активации необходимо добавить в хранилище Сервера администрирования.

Инструкции:

- Консоль администрирования:
  - Добавление лицензионного ключа в хранилище Сервера администрирования.
  - Автоматическое распространение лицензионного ключа.

  Или

- Kaspersky Security Center Web Console:
  - Добавление лицензионного ключа в хранилище Сервера администрирования
  - Автоматическое распространение лицензионного ключа.

Обратите внимание, что автоматически распространяемый лицензионный ключ может не отображаться в хранилище виртуального Сервера администрирования в следующих случаях:

- Лицензионный ключ недействителен для приложения.
- Виртуальный Сервер администрирования не имеет управляемых устройств.
- Лицензионный ключ уже используется для устройств, управляемых другим виртуальным Сервером администрирования, и достигнуто лицензионное ограничение на количество устройств.

Добавление файла ключа или кода активации в инсталляционный пакет управляемого приложения

Из соображений безопасности не рекомендуется использовать этот параметр. Файл ключа или код активации, добавленный в инсталляционный пакет, может быть скомпрометирован.

В случае установки управляемого приложения с помощью инсталляционного пакета вы можете указать код активации или файл ключа в инсталляционном пакете или в политике этого приложения. Лицензионный ключ распространится на управляемые устройства при очередной синхронизации устройства с Сервером администрирования.

Инструкции:

- Консоль администрирования:
  - Создание инсталляционного пакета.
  - Установка приложений на клиентские устройства.

  Или

- Kaspersky Security Center Web Console: Добавление лицензионного ключа в инсталляционный пакет.

Распространение с помощью задачи добавления лицензионного ключа управляемого приложения

В случае использования задачи *Добавление лицензионного ключа* управляемого приложения вы можете выбрать лицензионный ключ, который необходимо распространить на устройства, и выбрать устройства удобным вам способом, например, выбрав группу администрирования или выборку устройств.

Перед распространением файл ключа или код активации необходимо добавить в хранилище Сервера администрирования.

Инструкции:

- Консоль администрирования:
  - Добавление лицензионного ключа в хранилище Сервера администрирования.
  - Распространение лицензионного ключа на клиентские устройства.

  Или
- Kaspersky Security Center Web Console:
  - Добавление лицензионного ключа в хранилище Сервера администрирования
  - Распространение лицензионного ключа на клиентские устройства.

Добавление кода активации или файла ключа вручную на устройства

Вы можете активировать установленное приложение "Лаборатории Касперского" локально, используя инструменты приложения. Дополнительную информацию см. в документации к установленным приложениям.

Добавление лицензионного ключа в хранилище Сервера администрирования

Чтобы добавить лицензионный ключ в хранилище Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.
2. Нажмите на кнопку **Добавить**.
3. Выберите то, что вы хотите добавить:
   - **Добавить файл ключа**

     Нажмите на кнопку **Выберите файл ключа** и выберите файл .key, который вы хотите добавить.

- **Ввести код активации**

  Укажите код активации в текстовом поле и нажмите на кнопку **Отправить**.

4. Нажмите на кнопку **Закрыть**.

Лицензионный ключ или несколько лицензионных ключей добавлены в хранилище Сервера администрирования.

Добавление лицензионного ключа Сервера администрирования

Чтобы добавить лицензионный ключ Сервера администрирования:

1. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
2. В открывшемся окне свойств Сервера администрирования выберите раздел **Лицензионные ключи**.
3. В разделе **Активный лицензионный ключ** нажмите на кнопку **Изменить**.
4. В открывшемся окне добавьте лицензионный ключ, нажав на кнопку **Добавить**.

   Запустится мастер добавления лицензионного ключа.

После завершения работы мастера вы можете проверить, отображаются ли функции в Консоли администрирования согласно соответствующей лицензией.

Распространение лицензионного ключа на клиентские устройства

Kaspersky Security Center Web Console позволяет распространить лицензионный ключ на клиентские устройства автоматически или с помощью задачи **Активация приложения**. Вы можете использовать задачу для распространения ключей в определенной группе устройств. При распространении лицензионного ключа с помощью задачи учитывается лицензионное ограничение на количество устройств. Используйте автоматическое распространение ключей, чтобы автоматически прекратить распространение лицензионного ключа при достижении лицензионного ограничения.

Если вы включили автоматическое распространение лицензионного ключа, не создавайте задачу **Активация приложения** для распространения этого ключа на клиентские устройства. Иначе нагрузка на Сервер администрирования увеличится из-за частой синхронизации.

Перед распространением добавьте лицензионный ключ в хранилище Сервера администрирования.

*Чтобы распространить лицензионный ключ на клиентские устройства с помощью задачи **Активация приложения**:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится **мастер создания задачи**. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. В раскрывающемся списке **Приложение** выберите приложение, для которого вы хотите добавить лицензионный ключ.

4. В списке **Тип задачи** выберите задачу **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 позволяет автоматически распространять на управляемые устройства лицензионные ключи, размещенные в хранилище ключей на Сервере администрирования.

Чтобы автоматически распространять лицензионный ключ на управляемые устройства:

1. В главном окне приложения перейдите в раздел **Операции → Лицензирование → Лицензии "Лаборатории Касперского"**.

2. Нажмите на имя лицензионного ключа, который вы хотите автоматически распространять на устройства.

3. В открывшемся окне свойств лицензионного ключа установите флажок **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.

Виртуальный Сервер администрирования автоматически распространяет лицензионные ключи из своего хранилища и из хранилища Сервера администрирования. Рекомендуется:

- Используйте задачу *Добавить лицензионный ключ*, чтобы выбрать лицензионный ключ, который необходимо развернуть на устройствах.
- Не выключайте параметр **Разрешить автоматическое распространение лицензионных ключей этого виртуального Сервера на его устройства** в параметрах виртуального Сервера администрирования. Иначе виртуальный Сервер администрирования не будет распространять лицензионные ключи на устройства, в том числе лицензионные ключи из хранилища Сервера администрирования.

Если установлен флажок **Автоматически распространять лицензионный ключ на управляемые устройства** в окне свойств лицензионного ключа, лицензионный ключ будет немедленно распространен в вашей сети. Если вы не выберете этот параметр, вы можете использовать задачу распространения лицензионного ключа позже.

Автоматическое распространение лицензионных ключей, настроенных на главном Сервере администрирования, не включает устройства, управляемые невиртуальными подчиненными Серверами администрирования.

Просмотр информации об используемых лицензионных ключах

Чтобы просмотреть список лицензионных ключей, добавленных в хранилище Сервера администрирования:

В главном окне приложения перейдите в раздел **Операции → Лицензирование → Лицензии "Лаборатории Касперского"**.

Отобразится список файлов ключей и кодов активации, добавленных в хранилище Сервера администрирования.

Чтобы просмотреть подробную информацию о лицензионном ключе:

1. В главном окне приложения перейдите в раздел **Операции → Лицензирование → Лицензии "Лаборатории Касперского"**.
2. Нажмите на имя требуемого лицензионного ключа.

В открывшемся окне свойств лицензионного ключа вы можете просмотреть:

- На вкладке **Общие** – основную информацию о лицензионном ключе.
- На вкладке **Устройства** – список клиентских устройств, на которых использовался лицензионный ключ для активации установленного приложения "Лаборатории Касперского".

Чтобы просмотреть, какие лицензионные ключи распространены на выбранное клиентское устройство:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. Нажмите на имя требуемого устройства.
3. В открывшемся окне свойств устройства выберите вкладку **Приложения**.
4. Нажмите на название приложения, для которого вы хотите просмотреть информацию о распространенном лицензионном ключе.
5. В открывшемся окне свойств приложения перейдите на вкладку **Общие** и откройте раздел **Лицензия**.

Отобразится основная информация об активных и резервных лицензионных ключах.

Для определения актуальных параметров лицензионных ключей виртуального Сервера администрирования Сервер администрирования отправляет запрос на серверы активации "Лаборатории Касперского" не реже одного раза в сутки. Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы.

Удаление лицензионного ключа из хранилища

При удалении активного лицензионного ключа для дополнительной возможности Сервера администрирования, например, для возможности Системного администрирования или Управления мобильными устройствами, соответствующая функциональность становится недоступной. Если был добавлен резервный лицензионный ключ, резервный лицензионный ключ автоматически становится активным лицензионным ключом после удаления предыдущего активного лицензионного ключа.

При удалении активного лицензионного ключа, который распространен на управляемые устройства, приложения продолжают работать на управляемых устройствах.

Чтобы удалить файл ключа или код активации из хранилища Сервера администрирования:

1. Убедитесь, что Сервер администрирования не использует файл ключа или код активации, который вы намерены удалить. Если Сервер администрирования использует такой ключ, вы не сможете удалить ключ. Чтобы выполнить проверку:

   a. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

b. На вкладке **Общие** выберите раздел **Лицензионные ключи**.

c. Если в открывшемся разделе отображается требуемый файл ключ или код активации, нажмите на кнопку **Удалить активный лицензионный ключ** и подтвердите операцию. После этого Сервер администрирования не использует удаленный лицензионный ключ, ключ остается в хранилище Сервера администрирования. Если требуемый файл ключ или код активации не отображается, Сервер администрирования его не использует.

2. В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.

3. Выберите нужный файл ключа или код активации и нажмите на кнопку **Удалить**.

Выбранный файл ключа или код активации удален из хранилища.

Можно добавить удаленный лицензионный ключ повторно или добавить другой лицензионный ключ.

Отзыв согласия с Лицензионным соглашением

Если вы решите прекратить защиту некоторых своих клиентских устройств, вы можете отозвать Лицензионное соглашение для любого управляемого приложения "Лаборатории Касперского". Вам нужно удалить выбранное приложение, прежде чем отзывать его Лицензионное соглашение.

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. Откройте окно свойств Сервера администрирования и на вкладке **Общие** выберите раздел **Лицензионные соглашения**.

   Отобразится список Лицензионных соглашений, принятых при создании инсталляционных пакетов, установке обновлений или развертывании Kaspersky Security для мобильных устройств.

2. В списке выберите Лицензионные соглашения, которые вы хотите отозвать.

   Можно просмотреть следующие свойства Лицензионных соглашений:

   - Дата принятия Лицензионного соглашения.
   - Имя пользователя, принявшего Лицензионное соглашение.

3. Нажмите на дату принятия любого Лицензионного соглашения, чтобы открыть окно его свойств, в котором отображаются следующие данные:

   - Имя пользователя, принявшего Лицензионное соглашение.
   - Дата принятия Лицензионного соглашения.
   - Уникальный идентификатор (UID) Лицензионного соглашения.

- Полный текст Лицензионного соглашения.
- Список объектов (инсталляционных пакетов, обновлений, мобильных приложений), связанных с Лицензионным соглашением, и их соответствующие имена и типы.

4. В нижней части окна свойств Лицензионного соглашения нажмите на кнопку **Отозвать Лицензионное соглашение**.

   Если существуют какие-либо объекты (инсталляционные пакеты и их соответствующие задачи), которые не позволяют отозвать Лицензионное соглашение, отображается соответствующее уведомление. Вы не можете продолжить отзыв, пока не удалите эти объекты.

   В открывшемся окне отобразится сообщение о том, что сначала необходимо удалить приложение "Лаборатории Касперского", которому соответствует это Лицензионное соглашение.

5. Нажмите на кнопку, подтверждающую отзыв лицензии.

Лицензионное соглашение отозвано. Лицензионное соглашение больше не отображается в списке Лицензионных соглашений в разделе **Лицензионные соглашения**. Окно свойств Лицензионного соглашения закрывается; приложение больше не установлено.

Продление срока действия лицензии приложений "Лаборатории Касперского"

Вы можете продлить срок действия лицензии приложений "Лаборатории Касперского", срок действия которой истек или скоро истечет (менее чем через 30 дней).

Чтобы продлить срок действия лицензии, который истекает или уже истек:

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Операции → Лицензирование → Лицензии "Лаборатории Касперского"**.
   - В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Панель мониторинга** и перейдите по ссылке **Просмотреть лицензии, срок действия которых истек** рядом с уведомлением.

   Откроется окно **Лицензии "Лаборатории Касперского"**, в котором вы можете просмотреть и продлить срок действия лицензии.

2. Перейдите по ссылке **Продлить срок действия лицензии** рядом с требуемой лицензией.

   Нажимая на ссылку продления срока действия лицензии, вы соглашаетесь передавать в "Лабораторию Касперского" следующие данные Kaspersky Security Center: версию, локализацию, которую вы используете, идентификатор лицензии на программное обеспечение (то есть идентификатор лицензии, которую вы продлеваете), а также то, приобрели ли вы лицензию через компанию-партнера или нет.

3. В открывшемся окне продления срока действия лицензии следуйте инструкциям.

   Срок действия лицензии продлен.

В Kaspersky Security Center Web Console уведомления отображаются при приближении истечения срока действия лицензии по следующему расписанию:

- за 30 дней до истечения срока действия;
- за 7 дней до истечения срока действия;
- за 3 дней до истечения срока действия;
- за 24 часа до истечения срока действия;
- когда срок действия лицензии истек.

Использование Kaspersky Marketplace для выбора бизнес-решений

Marketplace – раздел главного меню, позволяющий просмотреть весь спектр бизнес-решений "Лаборатории Касперского", выбрать те, которые вам нужны, и перейти к покупке на сайте "Лаборатории Касперского". Вы можете использовать фильтры для просмотра только тех решений, которые соответствуют вашей организации и требованиям вашей системы информационной безопасности. Когда вы выбираете решение, Kaspersky Security Center перенаправляет вас на соответствующую страницу на сайте "Лаборатории Касперского", чтобы вы могли узнать о решении подробнее. Каждая веб-страница позволяет вам перейти к покупке или содержит инструкции по процессу покупки.

В разделе **Marketplace** вы можете фильтровать решения "Лаборатории Касперского" по следующим критериям:

- Количество устройств (конечных точек, серверов и других типов активов), которые вы хотите защитить:
  - 50–250
  - 250–1000
  - Более 1000
- Уровень опытности команды информационной безопасности вашей организации:
  - **Foundations**

    Этот уровень типичен для предприятий, в которых есть только ИТ-команда. Максимально возможное количество угроз блокируется автоматически.
  - **Optimum**

    Этот уровень типичен для предприятий, у которых есть конкретная функция ИТ-безопасности в ИТ-команде. На этом уровне компаниям требуются решения, которые позволят им противостоять товарным угрозам и угрозам в обход существующих превентивных механизмов.
  - **Expert**

    Этот уровень типичен для предприятий со сложной и распределенной ИТ-средой. Группа ИТ-безопасности состоит из опытных специалистов, или в компании есть группа SOC (Security Operations Center). Необходимые решения позволяют компаниям противостоять комплексным угрозам и целевым атакам.

- Типы активов, которые вы хотите защитить:
  - **Конечные точки**: рабочие станции сотрудников, физические и виртуальные машины, встраиваемые системы.
  - **Серверы**: физические и виртуальные серверы.
  - **Cloud**: публичные, частные или гибридные облачные среды; облачные сервисы.
  - **Сеть**: локальная сеть, ИТ-инфраструктура.
  - **Услуга**: услуги, связанные с безопасностью, предоставляемые "Лабораторией Касперского".

Чтобы найти и приобрести бизнес-решение "Лабораторией Касперского":

1. В главном окне приложения перейдите в раздел **Marketplace**.

   По умолчанию в разделе отображаются все доступные бизнес-решения "Лаборатории Касперского".

2. Чтобы просмотреть только те решения, которые подходят вашей организации, выберите нужные значения в фильтрах.

3. Нажмите на решение, которое вы хотите приобрести или о котором хотите узнать больше.

   Вы будете перенаправлены на веб-страницу решения. Следуйте инструкциям на экране, чтобы перейти к покупке.

Настройка защиты сети

В этом разделе содержится информация о настройке вручную политик и задач, о ролях пользователей, о построении структуры групп администрирования и об иерархии задач.

Сценарий: настройка защиты сети

Мастер первоначальной настройки создает политики и задачи с параметрами по умолчанию. Эти параметры могут оказаться не оптимальными или даже запрещенными в организации. Поэтому рекомендуется настроить эти политики и задачи и создать дополнительные политики и задачи, если это необходимо для вашей сети.

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- Установили Сервер администрирования Kaspersky Security Center.
- Установили Kaspersky Security Center Web Console (если требуется).
- Выполнили основной сценарий установки Kaspersky Security Center.

- Мастер первоначальной настройки завершен или следующие политики и задачи созданы вручную в группе администрирования **Управляемые устройства**:
  - политика Kaspersky Endpoint Security;
  - групповая задача обновления Kaspersky Endpoint Security;
  - политика Агента администрирования;
  - задача *Поиск уязвимостей и требуемых обновлений*.

Настройка защиты сети состоит из следующих этапов:

1. **Настройка и распространение политик и профилей политик для приложений "Лаборатории Касперского"**

   Для настройки и распространения параметров приложений "Лаборатории Касперского", установленных на управляемых устройствах, можно использовать два различных подхода управления безопасностью: ориентированный на пользователей и ориентированный на устройства. Можно комбинировать эти два подхода. Для реализации ориентированного на устройства метода управления безопасностью подходят средства Консоли администрирования на основе консоли управления Microsoft Management Console (MMC) и Kaspersky Security Center Web Console. Для реализации ориентированного на пользователей метода управления безопасностью подходит только Kaspersky Security Center Web Console.

2. **Настройка задач для удаленного управления приложениями "Лаборатории Касперского"**

   Проверьте задачи, созданные с помощью мастера первоначальной настройки, и при необходимости оптимизируйте их параметры.

   Инструкции:

   - Консоль администрирования:
     - Настройка групповой задачи обновления Kaspersky Endpoint Security.
     - Настройка расписания задачи Поиск уязвимостей и требуемых обновлений.
   - Kaspersky Security Center Web Console:
     - Настройка групповой задачи обновления Kaspersky Endpoint Security.
     - Параметры задачи поиска 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:

   - Консоль администрирования: Настройка максимального количества событий.
   - Kaspersky Security Center Web Console: Настройка максимального количества событий.

Результаты

После завершения этого сценария ваша сеть будет защищена благодаря настройке приложений "Лаборатории Касперского", задач и событий, получаемых Сервером администрирования:

- приложения "Лаборатории Касперского" настроены в соответствии с политиками и профилями политик.
- Управление приложениями осуществляется с помощью набора задач.
- Задано максимальное количество событий, которые могут храниться в базе данных.

После завершения настройки защиты сети вы можете приступить к настройке регулярных обновлений баз и приложений "Лаборатории Касперского".

Подробнее о настройке автоматического ответа на угрозы, обнаруженных Kaspersky Sandbox, см. в справке Kaspersky Sandbox 2.0.

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. Для реализации ориентированного на устройства метода управления безопасностью подходят средства Консоли администрирования на основе консоли управления Microsoft Management Console (MMC) и Kaspersky Security Center Web Console. Для реализации ориентированного на пользователей метода управления безопасностью подходит только Kaspersky Security Center Web Console.

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

После завершения этого сценария приложения будут настроены на всех управляемых устройствах в соответствии с политиками приложений и профилями политики, которые вы определяете.

Предварительные требования

Убедитесь, что вы установили Сервер администрирования Kaspersky Security Center и Kaspersky Security Center Web Console (если требуется). Если вы установили Kaspersky Security Center Web Console, вам может быть интересно также управление безопасностью, ориентированное на пользователей, в качестве альтернативы или дополнения к управлению безопасностью, ориентированному на устройства.

Этапы

Сценарий управления приложениями "Лаборатории Касперского", ориентированный на устройства, содержит следующие шаги:

1. **Настройка политик приложений**

   Настройте параметры установленных приложений "Лаборатории Касперского" на управляемых устройствах с помощью создания политики для каждого приложения. Этот набор политик будет применен к клиентским устройствам.

   При настройке защиты сети с помощью мастера первоначальной настройки Kaspersky Security Center создает политику по умолчанию для следующих приложений:

   - Kaspersky Endpoint Security для Windows – для клиентских устройств с операционной системой Windows.
   - Kaspersky Endpoint Security для Linux – для клиентских устройств с операционной системой Linux.

   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 Серверов администрирования и/или групп администрирования, подчиненные Серверы администрирования и дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами и подчиненными Серверами администрирования, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их выше по иерархии политики. Остальные незаблокированные параметры будут доступны для изменения в политике ниже по иерархии. Созданная иерархия политик позволяет эффективно управлять устройствами в группах администрирования.

Инструкции:

- Консоль администрирования: Создание политики.
- Kaspersky Security Center Web Console: 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:

- Консоль администрирования:
  - Создание профиля политики.
  - Создание правила активации профиля политики.
- Kaspersky Security Center Web Console:
  - Создание профиля политики.
  - Создание правила активации профиля политики.

3. **Распространение политик и профилей политик на управляемые устройства**

По умолчанию синхронизация управляемых устройств с Сервером администрирования происходит раз в 15 минут. Вы можете пропустить автоматическую синхронизацию и запустить синхронизацию вручную с помощью команды Синхронизировать принудительно. Также принудительная синхронизация выполняется после создания или изменения политики или профиля политики. Во время синхронизации новые или измененные политики и профили политик применяются к управляемым устройствам.

Если вы используете Kaspersky Security Center Web Console, можно проверить, доставлены ли политики и профили политик на устройства. Kaspersky Security Center определяет дату и время доставки в свойствах устройства.

Инструкции:

- Консоль администрирования: Принудительная синхронизация.
- Kaspersky Security Center Web Console: 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.

> Этот сценарий можно реализовать с помощью Kaspersky Security Center Web Console версии 13 и выше.

Предварительные требования

Убедитесь, что вы успешно установили Сервер администрирования Kaspersky Security Center и Kaspersky Security Center Web Console и завершили основной сценарий установки. 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 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 Серверов администрирования и/или групп администрирования, подчиненные Серверы администрирования и дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами и подчиненными Серверами администрирования, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их выше по иерархии политики. Остальные незаблокированные параметры будут доступны для изменения в политике ниже по иерархии. Созданная иерархия политик позволяет эффективно управлять устройствами в группах администрирования.

Инструкция: Создание политики.

2. **Укажите пользователей в качестве владельцев устройств**

   Назначьте управляемым устройствам соответствующих пользователей.

   Инструкция: Назначение пользователя владельцем устройства.

3. **Определение пользовательских ролей, типичных для вашей организации**

   Подумайте о различных видах работ, которые обычно выполняют сотрудники вашей организации. Вам нужно разделить всех сотрудников в соответствии с их ролями. Например, вы можете разделить их по отделам, профессиям или должностям. После этого вам потребуется создать роль пользователя для каждой группы. В этом случае каждая пользовательская роль будет иметь свой собственный профиль политики, содержащий параметры приложения, специфичные для этой роли.

4. **Создание пользовательских ролей**

   Создайте и настройте пользовательскую роль для каждой группы сотрудников, которую вы определили на предыдущем шаге, или используйте предопределенные роли. Роли пользователей содержат набор прав доступа к функциям приложения.

   Инструкция: Создание роли пользователя.

5. **Определение области для каждой роли пользователя**

   Для каждой созданной роли пользователя определите пользователей и/или группы безопасности и группы администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

   Инструкция: Изменение области для роли пользователя.

6. **Создание профилей политики**

   Создайте профиль политики для каждой роли пользователя вашей организации. Профили политики определяют, какие параметры должны применяться к приложениям, установленным на устройствах пользователей, в зависимости от роли каждого пользователя.

   Инструкция: Создание профиля политики.

7. **Связь профиля политики с ролями пользователей**

   Свяжите созданные профили политики с ролями пользователей. После чего, профиль политики становится активным для пользователей, которым определена эта роль. Параметры профиля политики, применяются к приложениям "Лаборатории Касперского", установленным на устройствах пользователя.

   Инструкция: Связь профилей политики с ролями.

8. **Распространение политик и профилей политик на управляемые устройства**

По умолчанию синхронизация управляемых устройств с Сервером администрирования происходит раз в 15 минут. Во время синхронизации новые или измененные политики и профили политик применяются к управляемым устройствам. Вы можете пропустить автоматическую синхронизацию и запустить синхронизацию вручную с помощью команды Синхронизировать принудительно. После завершения синхронизации политики и профили политик доставляются и применяются к установленным приложениям "Лаборатории Касперского".

Вы можете проверить, доставлены ли политики и профили политик на устройство. Kaspersky Security Center определяет дату и время доставки в свойствах устройства.

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 **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на название политики Агента администрирования.

   Откроется окно свойств политики Агента администрирования.

См. таблицу сравнения, в которой подробно описано применение параметров, описанных ниже, в зависимости от используемой операционной системы.

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**

    Если выбран этот вариант, политика становится активной.

    По умолчанию выбран этот вариант.

- **Неактивна**

  Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.

- В блоке **Наследование параметров** можно настроить параметры наследования политики:

  - **Наследовать параметры родительской политики**

    Если параметр включен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

    По умолчанию параметр включен.

  - **Обеспечить принудительное наследование параметров для дочерних политик**

    Если параметр включен, после применения изменений в политике будут выполнены следующие действия:

    - значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
    - в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически включен параметр **Наследовать параметры родительской политики**.

    Когда параметр включен, значения параметров дочерних политик недоступны для изменения.

    По умолчанию параметр выключен.

Настройка событий

На этой вкладке можно настроить регистрацию событий и оповещение о событиях. События 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). После того как вы нажмете на тип события, можно настроить параметры регистрации и уведомления о событиях, выбранных в списке. По умолчанию общие настройки уведомлений, указанные для всего Сервера администрирования, используются для всех типов событий. Однако можно изменить определенные параметры для заданных типов событий.

Например, в разделе **Предупреждение**, вы можете настроить тип события **Произошла проблема безопасности**. Такие события могут произойти, например, когда свободное место на диске точки распространения меньше 2 ГБ (для установки приложений и удаленной загрузки обновлений требуется не менее 4 ГБ). Чтобы настроить событие **Произошла проблема безопасности**, нажмите на него и укажите, где хранить произошедшие события и как о них уведомлять.

Если Агент администрирования обнаружил проблему безопасности, вы можете управлять этой проблемой безопасности с помощью параметров управляемого устройства.

Параметры

В разделе **Параметры** можно настроить параметры политики Агента администрирования:

- **Распространять файлы только через точки распространения**

  Если этот параметр включен, Агенты администрирования на управляемых устройствах получают обновления только от точек распространения.

  Если этот параметр выключен, Агенты администрирования на управляемых устройствах получают обновления от точек распространения или от Сервера администрирования.

  > Обратите внимание, что приложения безопасности на управляемых устройствах получают обновления от источника, заданного в задаче обновления для каждого приложения безопасности. Если вы включили параметр **Распространять файлы только через точки распространения**, убедитесь, что Kaspersky Security Center установлен в качестве источника обновлений в задачах обновления.

  По умолчанию параметр выключен.

- **Максимальный размер очереди событий (МБ)**

  В поле можно указать максимальное место на диске, которое может занимать очередь событий.

  По умолчанию указано значение 2 МБ.

- **Приложение может получать расширенные данные политики на устройстве**

  Агент администрирования, установленный на управляемом устройстве, передает информацию о применяемой политике в приложение безопасности (например, Kaspersky Endpoint Security для 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.

  По умолчанию параметр выключен.

Хранилища

В разделе **Хранилища** можно выбрать типы объектов, информацию о которых Агент администрирования будет отправлять на Сервер администрирования. Если в политике Агента администрирования наложен запрет на изменение параметров, указанных в этом разделе, эти параметры недоступны для изменения.

- **Информация об установленных приложениях**

  Если этот параметр включен, на Сервер администрирования отправляется информация о приложениях, установленных на клиентских устройствах.

  По умолчанию параметр включен.

- **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**

  Установленный на устройстве Агент администрирования отправляет информацию об оборудовании устройства на Сервер администрирования. Вы можете просмотреть информацию об оборудовании в свойствах устройства.

  Убедитесь, что утилита lshw установлена на устройствах Linux, с которых вы хотите получить информацию об оборудовании. Сведения об оборудовании, полученные с виртуальных машин, могут быть неполными в зависимости от используемого гипервизора

Обновления и уязвимости в приложениях

В разделе **Обновления и уязвимости в приложениях** можно настроить поиск и распространение обновлений Windows, а также включить проверку исполняемых файлов на наличие уязвимостей:

- **Использовать Сервер администрирования в роли WSUS-сервера**

  Если этот параметр включен, обновления Windows загружаются на Сервер администрирования. Загруженные обновления Сервер администрирования централизованно предоставляет службам Windows Update на клиентских устройствах с помощью Агентов администрирования.

  Если этот параметр выключен, Сервер администрирования не используется для загрузки обновлений Windows. В этом случае клиентские устройства получают обновления Windows самостоятельно.

  По умолчанию параметр выключен.

- Вы можете ограничить обновления Центра обновления Windows, которые могут устанавливать пользователи на своих устройствах вручную, используя Центр обновления Windows.

  > Для устройств с операционными системами Windows 10, если в Центре обновления Windows уже найдены обновления для устройств, то новый параметр, который вы выбрали под **Разрешить пользователям управлять установкой обновлений Центра обновления Windows**, будет применен только после установки найденных обновлений.

  Выберите параметр из раскрывающегося списка:

  - **Устанавливать все применимые обновления Центра обновления Windows**

    Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам.

Выберите этот вариант, если вы не хотите влиять на установку обновлений.

Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

- **Устанавливать только одобренные обновления Центра обновления Windows**

  Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам и которые одобрены администратором.

  Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом разрешить установку этих одобренных обновлений на клиентских устройствах.

  Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

- **Запретить устанавливать обновления Центра обновления Windows**

  Пользователи не могут устанавливать обновления Центра обновления Windows на своих устройства вручную. Все применимые обновления устанавливаются в соответствии с настройкой, заданной администратором.

  Выберите этот вариант, если вы хотите централизованно управлять установкой обновлений.

  Например, вы можете настроить расписание обновления так, чтобы не загружать сеть. Вы можете запланировать обновления вне рабочего времени, чтобы они не мешали производительности пользователей.

- 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 включен.

Управление перезагрузкой

В разделе **Управление перезагрузкой** можно выбрать и настроить действие, если во время работы, установки или удаления приложения требуется перезагрузить операционную систему управляемого устройства:

- **Не перезагружать операционную систему**

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **При необходимости перезагрузить операционную систему автоматически**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

  - **Повторять запрос периодически через (мин)**

    Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

    По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

    Если параметр выключен, предложение перезагрузки отображается только один раз.

  - **Принудительно перезагружать через (мин)**

    После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать приложения в заблокированных сеансах**

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.

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:

- **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.

  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:

- **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**

  Если флажок установлен, патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений.

  Если флажок снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрен*.

  По умолчанию параметр включен.

- **Загружать обновления и антивирусные базы с Сервера администрирования заранее (рекомендуется)**

  Если параметр включен, офлайн-модель получения обновлений используется. Когда Сервер администрирования получает обновления, он уведомляет Агент администрирования (на устройствах, где он установлен) об обновлениях, которые потребуются для управляемых приложений. Когда Агенты администрирования получают информацию об обновлениях, они загружают нужные файлы с Сервера администрирования заранее. При первом соединении с Агентом администрирования Сервер инициирует загрузку обновлений этим Агентом. После того как Агент администрирования на клиентском устройстве загрузит все обновления, обновления становятся доступными для приложений на устройстве.

  Когда управляемое приложение на клиентском устройстве обращается к Агенту администрирования за обновлениями, Агент проверяет, есть ли у него необходимые обновления. Если обновления были получены от Сервера администрирования не раньше, чем за 25 часов с момента запроса управляемого приложения, Агент администрирования не подключается к Серверу администрирования и предоставляет управляемому приложению обновления из локального кеша. Соединение с Сервером администрирования может не выполняться, когда Агент администрирования предоставляет обновления для приложений на клиентских устройствах, но подключение не требуется для обновления.

  Если параметр выключен, офлайн-модель получения обновлений не используется. Обновления распространяются в соответствии с расписанием задачи загрузки обновлений.

  По умолчанию параметр включен.

Подключения

Раздел **Подключения** включает три вложенных раздела:

- **Сеть**
- **Профили соединений**
- **Расписание соединений**

В разделе **Сеть** можно настроить параметры подключения к Серверу администрирования, включить возможность использования UDP-порта и указать его номер.

- В блоке **Подключиться к Серверу администрирования** можно настроить параметры подключения к Серверу администрирования и указать период синхронизации клиентских устройств с Сервером администрирования:

  - **Период синхронизации (мин)**

    Агент администрирования синхронизирует управляемые устройства с Сервером администрирования. Рекомендуется задать период синхронизации (периодический сигнал) равным 15 минут на 10 000 управляемых устройств.

  - **Сжимать сетевой трафик**

    Если параметр выключен, будет увеличена скорость передачи данных Агентом администрирования, сокращен объем передаваемой информации и уменьшена нагрузка на Сервер администрирования.

    > Нагрузка на центральный процессор клиентского компьютера может возрасти.

    По умолчанию флажок установлен.

  - **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**

    Если параметр включен, порты, необходимые для работы Агента администрирования и Сервера администрирования, будут добавлены в список исключений брандмауэра Microsoft Windows.

    По умолчанию параметр включен.

  - **Использовать SSL-соединение**

    Если этот параметр включен, подключение к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

    По умолчанию параметр включен.

  - **Использовать шлюз соединения точки распространения (при наличии) в параметрах подключения по умолчанию**

    Если параметр включен, то используется шлюз соединений точки распространения, параметры которой заданы в свойствах группы администрирования.

    По умолчанию параметр включен.

- **Использовать UDP-порт**

  Чтобы Агент администрирования подключался к Серверу администрирования через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **Номер UDP-порт** укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к Серверу администрирования выполняется через UDP-порт 15000.

- **Номер UDP-порта**

  В поле можно ввести номер UDP-порта. По умолчанию установлен порт 15000.

  Используется десятичная форма записи.

  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 вы выбрали параметр **Использовать эту точку распространения в качестве push-сервера** в окне параметров точки распространения. Иначе точка распространения не будет выполнять роль push-сервера.

В подразделе **Профили соединений** можно задать параметры сетевого местоположения и включить автономный режим, когда Сервер администрирования недоступен:

- **Параметры сетевого местоположения**

  Параметры сетевого местоположения определяют характеристики сети, к которой подключено клиентское устройство, и задают правила переключения Агента администрирования с одного профиля подключения Сервера администрирования на другой при изменении характеристик сети.

- **Профили подключения к Серверу администрирования**

  В этом разделе можно просмотреть и добавить профили подключения Агента администрирования к Серверу администрирования. В этом разделе также можно сформировать правила переключения Агента администрирования на другие Серверы администрирования при возникновении следующих событий:

  - подключении клиентского устройства к другой локальной сети;
  - отключении устройства от локальной сети организации;
  - изменении адреса шлюза соединения или изменении адреса DNS-сервера.

  > Профили подключения поддерживаются только для устройств под управлением Windows и macOS.

- **Включить автономный режим, когда Сервер администрирования недоступен**

  Если параметр включен, при подключении через этот профиль приложения, установленные на клиентском устройстве, будут использовать профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей. В случае, если для приложения политика для автономных пользователей не определена, приложение будет использовать активную политику.

  Если параметр выключен, приложения будут использовать активные политики.

  По умолчанию параметр выключен.

В разделе **Расписание соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования:

- **Подключаться при необходимости**

  Если выбран этот вариант, подключение будет устанавливаться тогда, когда Агенту администрирования нужно передать данные на Сервер администрирования.

  По умолчанию выбран этот вариант.

- **Подключаться в указанные периоды**

  Если выбран этот вариант, подключение Агента администрирования к Серверу администрирования выполняется в заданные периоды времени. Можно добавить несколько периодов подключения.

Опрос сети точками распространения

В разделе **Опрос сети точками распространения** вы можете настроить автоматический опрос сети. Вы можете использовать следующие параметры, чтобы включить опрос и настроить его расписание:

- **Сеть Windows**

  Если этот параметр включен, Сервер администрирования автоматически опрашивает сеть в соответствии с расписанием, настроенным по ссылкам **Настроить расписание быстрого опроса** и **Настроить расписание полного опроса**.

  Если этот параметр выключен, Сервер администрирования опрашивает сеть с указанным периодом в поле **Период опроса сети (мин)**.

  Период обнаружения устройств для версий Агента администрирования ниже 10.2 можно настроить в полях **Период опроса Windows-доменов (мин)** (для быстрого опроса сети Windows) и **Период опроса сети (мин)** (для полного опроса сети Windows).

  По умолчанию параметр выключен.

- **Zeroconf**

  Если этот параметр включен, точка распространения автоматически опрашивает сеть с устройствами IPv6, используя сеть с нулевой конфигурацией (далее также *Zeroconf*). В этом случае включенный опрос IP-диапазонов игнорируется, так как точка распространения опрашивает всю сеть.

  Чтобы можно было начать использовать Zeroconf, должны быть выполнены следующие условия:

  - Точка распространения должна работать под управлением Linux.
  - Вам нужно установить утилиту avahi-browse на точку распространения.

  Если этот параметр отключен, точка распространения не опрашивает сети с устройствами IPv6.

  По умолчанию параметр выключен.

- **IP-диапазоны**

  Если этот параметр включен, точка распространения автоматически опрашивает IP-диапазоны в соответствии с расписанием, настроенным по кнопке **Настроить расписание опроса**.

  Если параметр выключен, точка распространения не выполняет опрос IP-диапазонов.

  Периодичность опроса IP-диапазонов для версий Агента администрирования версий ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если параметр включен.

По умолчанию параметр выключен.

- **Контроллеры доменов**

  Если этот параметр включен, точка администрирования автоматически выполняет опрос Active Directory в соответствии с расписанием, настроенным по ссылке **Настроить расписание опроса**.

  Если параметр выключен, Сервер администрирования не выполняет опрос Active Directory.

  Периодичность опроса Active Directory для версий Агента администрирования версий ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если этот параметр включен.

  По умолчанию параметр выключен.

  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

Если ваши точки распространения используют прокси-сервер для подключения к интернету, в подразделе **Параметры сети для точек распространения** вы можете указать следующие параметры:

- **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 Kaspersky Security Network (KSN) запросов от управляемых устройств:

- **Включить прокси-сервер KSN на стороне точки распространения**

  Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

  Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского".

  По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены в окне свойств Сервера администрирования.

  Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

- **Пересылать KSN запрос Серверу администрирования**

  Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

  По умолчанию параметр включен.

- **Доступ к облачной службе KSN/KPSN непосредственно через интернет**

  Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или KPSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или KPSN.

  Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к KPSN. Если вы хотите перенастроить точки распространения для отправки запросов KSN в KPSN, включите параметр **Пересылать KSN запрос Серверу администрирования** для каждой точки распространения.

  Точки распространения с установленным Агентом администрирования версии 12 (и выше) могут напрямую обращаться к KPSN.

- **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.

Обновления (точки распространения)

В разделе **Обновления (точки распространения)** вы можете включить функцию загрузки файлов различий, так как точки распространения получают обновления в виде файлов различий с серверов обновлений "Лаборатории Касперского".

Управление учетными записями (только для Linux)

Раздел **Управление учетными записями (только для Linux)** состоит из трех подразделов:

- **Управление пользовательскими сертификатами**
- **Добавление или изменение групп локальных администраторов**
- **Загрузка референсного файла, для защиты файла sudoers на устройстве пользователя от изменений**

В подразделе **Управление пользовательскими сертификатами** вы можете указать, какие корневые сертификаты устанавливать. Эти сертификаты могут использоваться, например, для проверки подлинности веб-сайтов или веб-серверов.

- **Установить корневые сертификаты**

  Если этот параметр включен, сертификаты, добавленные в таблицу, будут установлены на указанных устройствах.

  Если этот параметр выключен, сертификаты не будут установлены на указанные устройства.

  По умолчанию параметр выключен.

- **Добавить**

  Нажав на эту кнопку открывается окно, в котором можно добавить сертификат.

  Размер сертификата должен быть меньше 10 МБ.

  Kaspersky Security Center поддерживает сертификаты с расширениями CER, CRT, CERT, PEM и KEY.

В подразделе **Добавление или изменение групп локальных администраторов** вы можете управлять группами локальных администраторов. Эти группы используются, например, при отзыве прав локального администратора. Вы также можете проверить список учетных записей привилегированных пользователей, используя **Отчет о привилегированных пользователях устройств (только для Linux)**.

- **Добавить**

  Нажмите на эту кнопку, чтобы добавить локальную группу администраторов.

- **Изменить**

  Нажмите на эту кнопку, чтобы изменить локальную группу администраторов.

  Эта кнопка доступна, если установлен флажок рядом с группой локальных администраторов.

- **Удалить**

  Нажмите на эту кнопку, чтобы удалить выбранную группу локальных администраторов из таблицы.

Эта кнопка доступна, если установлен флажок рядом с группой локальных администраторов.

В подразделе **Загрузка референсного файла, для защиты файла sudoers на устройстве пользователя от изменений** вы можете настроить управление файлом sudoers. Привилегированные группы и пользователи устройства определяются файлом sudoers на устройстве. Файл sudoers находится в папке `/etc/sudoers`. Вы можете загрузить референсный файл sudoers, чтобы защитить файл sudoers от изменений. Это предотвратит нежелательные изменения файла sudoers.

Недопустимый референсный файл sudoers может привести к неисправности устройства пользователя.

- **Контролировать файл sudoers**

  Если этот параметр включен, файл sudoers будет заменен текущим референсным файлом sudoers.

  Если этот параметр выключен, файл sudoers остается без изменений.

  По умолчанию параметр выключен.

- **Референсный файл sudoers**

  В этом поле отображается название загруженного референсного файла sudoers.

- **Загрузить**

  Нажмите на эту кнопку, чтобы загрузить референсный файл sudoers.

- **Текущий референсный файл sudoers**

  Нажмите на эту кнопку, чтобы просмотреть текущий файл sudoers.

История ревизий

На этой вкладке вы можете просмотреть список ревизий политики и изменения, для которых был выполнен откат.

Сравнение параметров политики Агента администрирования по операционным системам

В таблице ниже описано, какие параметры политики Агента администрирования можно использовать для настройки Агента администрирования в Консоли администрирования и в Kaspersky Security Center Web Console для определенной операционной системы.

Параметры политики Агента администрирования: сравнение по операционным системам

Раздел Политики	Windows	macOS	Linux
Общие	✓	✓	✓
Настройка событий	✓	✓	✓

Раздел Политики	Windows	macOS	Linux
Параметры	✓	✓	✓ Доступны следующие параметры: • **Распространять файлы только через точки распространения** • **Максимальный размер очереди событий (МБ)** • **Приложение может получать расширенные данные политики на устройстве**
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 параметра **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**.
Подключения → Профили соединений	✓	✓	—
Подключения → Расписание соединений	✓	✓	✓
Опрос сети точками распространения	✓ Доступны только параметры **Сеть Windows**, **IP-диапазоны** и **Контроллеры доменов**.	—	✓ Доступны следующие параметры: • **Zeroconf** • **IP-диапазоны** • **Контроллеры доменов**
Параметры сети для точек распространения	✓	✓	✓
Прокси-сервер KSN (точки распространения)	✓	—	✓
Обновления (точки распространения)	✓	—	✓
История ревизий	✓	✓	✓

Включение и выключение режима низкого потребления ресурсов для Агента администрирования

Режим низкого потребления ресурсов позволяет ограничить использование оперативной памяти Агента администрирования, установленного на клиентском устройстве. По умолчанию режим низкого потребления ресурсов выключен.

В режиме низкого потребления ресурсов не выполняются следующие функции:

- Агент администрирования не может быть назначен точкой распространения (вручную или автоматически).
- Агент администрирования не записывает информацию о состоянии Агента администрирования в отдельный текстовый файл.
- Агент администрирования не поддерживает офлайн-модель получения обновлений.
- Следующие компоненты и процессы выключены:
  - Получение информации о сторонних обновлениях и уязвимостях.
  - Запуск прокси-сервера KSN на стороне точки распространения.
  - Загрузка обновлений в хранилище точки распространения.
  - Не использование блокировки DNS-сервера.
  - Получение информации о свободном месте на диске.

Компоненты и процессы возобновляют работу после выключения режима низкого потребления ресурсов.

Чтобы включить режим низкого потребления ресурсов:

1. Выполните следующую команду в командной строке на клиентском устройстве:

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. Перезапустите Агент администрирования.
3. Чтобы проверить, включен ли режим низкого потребления ресурсов, в Windows откройте **Просмотр событий** и выберите **Журналы приложений и служб → Журнал событий Kaspersky Event Log**.

   Убедитесь, что в журнале событий есть такие события, как **Агент администрирования Kaspersky Security Center работает в режиме низкого потребления ресурсов**.

Режим низкого потребления ресурсов включен.

Чтобы выключить режим низкого потребления ресурсов:

1. Выполните следующую команду в командной строке на клиентском устройстве:

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. Перезапустите Агент администрирования.
3. Чтобы проверить, выключен ли режим низкого потребления ресурсов, в Windows откройте **Просмотр событий** и выберите **Журналы приложений и служб → Журнал событий Kaspersky Event Log**.

   Убедитесь, что последнее событие klnagent не содержит сообщение **Агент администрирования Kaspersky Security Center работает в режиме низкого потребления ресурсов**.

Режим низкого потребления ресурсов выключен.

Также можно включить режим низкого потребления ресурсов удаленно с помощью задачи *Удаленное выполнение скриптов*.

Настройка параметров защиты управляемых приложений

Для настройки параметров защиты управляемых приложений "Лаборатории Касперского" вы можете использовать политики.

Подробнее о настройке политик Kaspersky Endpoint Security см. в соответствующей справке:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux
- Справка Kaspersky Endpoint Security для Mac

Ручная настройка групповой задачи обновления Kaspersky Endpoint Security

Оптимальный и рекомендуемый вариант расписания для Kaspersky Endpoint Security **При загрузке обновлений в хранилище** при установленном флажке **Использовать автоматическое определение случайного интервала между запусками задачи**.

Удаленная деинсталляция приложений или обновлений программного обеспечения

Чтобы удаленно деинсталлировать приложения или обновления программного обеспечения:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для приложения Kaspersky Security Center выберите тип задачи **Удаленная деинсталляция приложения**.
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. Выберите, какое приложение вы хотите деинсталлировать, а затем выберите требуемые приложения, обновления или патчи, которые вы хотите удалить:

   - **Удалить управляемое приложение**

     Отображается список приложений "Лаборатории Касперского". Выберите приложение, которое вы хотите деинсталлировать.

   - **Удалить несовместимое приложение**

     Отобразится список приложений, несовместимых с приложениями безопасности "Лаборатории Касперского" или с Kaspersky Security Center. Установите флажки напротив приложений, которые требуется удалить.

   - **Удалить приложение из реестра приложений**

     По умолчанию Агенты администрирования отправляют на Сервер администрирования информацию о приложениях, установленных на управляемых устройствах. Список установленных приложений хранится в реестре приложений.

     Чтобы выбрать приложение из реестра приложений:

     a. Нажмите на поле **Приложение для деинсталляции** и выберите приложение, которое вы хотите деинсталлировать.

     > Если вы выбрали Агент администрирования Kaspersky Security Center, при запуске задачи статус *Завершено успешно* показывает, что процесс удаления запущен. При удалении Агента администрирования Kaspersky Security Center статус не меняется. В случае сбоя задачи статус меняется на *Сбой*.

     b. Укажите параметры деинсталляции:

        - **Способ удаления**

          Выберите, как вы хотите деинсталлировать приложение:

          - **Автоматически определять команду удаления**

            Если у приложения есть команда деинсталляции, заданная поставщиком приложения, Kaspersky Security Center использует эту команду. Рекомендуется выбрать этот вариант.

          - **Задать команду удаления**

            Выберите этот вариант, если вы хотите указать свою команду для деинсталляции приложения.

            > Рекомендуется сначала попробовать деинсталлировать приложение с помощью параметра **Автоматически определять команду удаления**. Если деинсталляция с помощью автоматически определенной команды не удалась, используйте свою команду.

            Введите команду установки в это поле и укажите следующий параметр:

            Используйте эту команду для удаления, только если команда по умолчанию не была обнаружена автоматически

Kaspersky Security Center проверяет, есть ли у выбранного приложения команда деинсталляции, заданная поставщиком приложения. Если команда найдена, Kaspersky Security Center будет использовать ее вместо команды, указанной в поле **Команда для удаления приложения**.

Рекомендуется включать этот параметр.

- **Выполнить перезагрузку после успешного удаления приложения**

  Если после деинсталляции приложения требуется перезагрузка операционной системы на управляемом устройстве, операционная система перезагружается автоматически.

- **Удалить указанное обновление приложения, патч или стороннее приложение**

  Отображается список обновлений, патчей и приложений сторонних производителей. Выберите объект, который вы хотите деинсталлировать.

  Отображаемый список представляет собой общий список приложений и обновлений, и он не соответствует приложениям и обновлениям, установленным на управляемых устройствах. Перед выбором объекта рекомендуется убедиться, что приложение или обновление установлено на устройствах, определенных в области действия задачи. В окне свойств можно просмотреть список устройств, на которых установлено приложение или обновление.

  Чтобы просмотреть список устройств:

  a. Нажмите на имя приложения или обновления.

     Откроется окно свойств.

  b. Откройте раздел **Устройства**.

     Вы также можете просмотреть список установленных приложений и обновлений в окне свойств устройства.

7. Укажите, как клиентские устройства будут загружать утилиту удаления:

- **С помощью Агента администрирования**

  Файлы доставляются на клиентские устройства Агентом администрирования, установленным на этих клиентских устройствах.

  Если этот параметр выключен, файлы доставляются с помощью инструментов Microsoft Windows.

  Рекомендуется включить этот параметр, если задача назначена для устройств с установленными Агентами администрирования.

- **Средствами операционной системы с помощью Сервера администрирования**

  Файлы передаются на клиентские устройства с использованием средств операционной системы Сервера администрирования. Этот параметр можно включить, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

- **Средствами операционной системы с помощью точек распространения**

  Файлы передаются на клиентские устройства с использованием инструментов операционной системы с помощью точек распространения. Этот параметр можно включить, если в сети есть хотя бы одна точка распространения.

  Если параметр **С помощью Агента администрирования** включен, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

- **Максимальное количество одновременных загрузок**

  Максимально допустимое количество клиентских устройств, на которые Сервер администрирования может одновременно передавать файлы. Чем больше это число, тем быстрее будет деинсталлировано приложение, но нагрузка на Сервер администрирования увеличивается.

- **Максимальное количество попыток деинсталляции**

  Если при запуске задачи *Удаленная деинсталляция приложения* Kaspersky Security Center не удается деинсталлировать приложение с управляемого устройства за указанное в параметрах количество запусков установок, Kaspersky Security Center прекращает доставку утилиты деинсталляции на это управляемое устройство и больше не запускает установщик на устройстве.

  Параметр **Максимальное количество попыток деинсталляции** позволяет вам сохранить ресурсы управляемого устройства, а также уменьшить трафик (деинсталляция, запуск файла MSI и сообщения об ошибках).

  Повторяющиеся попытки запуска задачи могут указывать на проблему на устройстве, которая препятствует деинсталляции. Администратор должен решить проблему за указанное количество попыток деинсталляции и перезапустить задачу (вручную или по расписанию).

  Если удаление не выполнено, проблема будет считаться неразрешимой и любые дальнейшие запуски считаются дорогостоящими с точки зрения нежелательного расхода ресурсов и трафика.

  После создания задачи, количество попыток установки равно `0`. Каждый запуск установки, который возвращает ошибку на устройстве, увеличивает показания счетчика.

  Если количество попыток деинсталляции, указанное в параметрах задачи, было превышено и устройство готово к деинсталляции приложения, вы можете увеличить значение параметра **Максимальное количество попыток деинсталляции** и запустить задачу деинсталляции приложения. Также вы можете создать другую задачу *Удаленная деинсталляция приложения*.

- **Предварительно проверять тип операционной системы перед загрузкой**

  Перед передачей файлов на клиентские устройства Kaspersky Security Center проверяет, применимы ли параметры утилиты установки к операционной системе клиентского устройства. Если параметры не применимы, Kaspersky Security Center не передает файлы и не пытается установить приложение. Например, чтобы установить некоторые приложения на устройства группы администрирования, в которую входят устройства с различными операционными системами, вы можете назначить задачу установки группе администрирования, а затем включить этот параметр, чтобы пропускать устройства с операционной системой, отличной от требуемой.

  При удаленной установке Агента администрирования на нераспределенные устройства Kaspersky Security Center или точка распространения автоматически определяет тип операционной системы устройства независимо от параметра **Предварительно проверять тип операционной системы перед загрузкой**.

- **Использовать пароль деинсталляции**

  Этот параметр отображается, если на предыдущем шаге вы выбрали **Удалить управляемое приложение** и указали Агент администрирования Kaspersky Security Center в поле **Приложение для деинсталляции**.

  Если вы ранее задавали пароль для удаленной деинсталляции Агента администрирования в параметрах политики Агента администрирования, установите флажок **Использовать пароль деинсталляции** и введите пароль для удаления в поле **Пароль**. Если вы не задавали пароль для удаленной деинсталляции Агента администрирования, не устанавливайте флажок.

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. Если необходимо, добавьте учетные записи, которые будут использоваться для запуска задачи удаленной деинсталляции:

   - **Учетная запись не требуется (Агент администрирования уже установлен)**

     Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор приложения. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

     Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

   - **Учетная запись требуется (Агент администрирования не используется)**

     Выберите этот вариант, если Агент администрирования не установлен на устройствах, для которых вы назначаете задачу *Удаленная деинсталляция приложения*. В этом случае вы можете указать учетную запись пользователя или SSH-сертификат для деинсталляции приложения.

     - **Локальная учетная запись**. Если выбран этот вариант, укажите учетную запись пользователя, от имени которой будет запускаться инсталлятор приложения. Нажмите на кнопку **Добавить**, выберите **Локальная учетная запись** и укажите данные учетной записи пользователя.

       Вы можете указать несколько учетных записей, если ни одна из них не обладает необходимыми правами на всех устройствах, для которых назначена задача. В этом случае для запуска задачи используются последовательно, сверху вниз, все добавленные учетные записи.

     - **SSH сертификат**. Если вы хотите деинсталлировать приложение с клиентского устройства под управлением Linux, вы можете указать SSH-сертификат вместо учетной записи пользователя. Нажмите на кнопку **Добавить**, выберите **SSH сертификат** и укажите закрытый и открытый ключи сертификата.

       Чтобы сгенерировать закрытый ключ, вы можете использовать утилиту ssh-keygen. Обратите внимание, что Kaspersky Security Center поддерживает формат закрытых ключей PEM, а утилита ssh-keygen по умолчанию генерирует SSH-ключи в формате OPENSSH. Формат OPENSSH не поддерживается Kaspersky Security Center. Чтобы создать закрытый ключ в поддерживаемом формате PEM, добавьте параметр -m PEM в команду ssh-keygen.

       Например:

       ```
       ssh-keygen -m PEM -t rsa -b 4096 -C "<электронная почта пользователя>"
       ```

10. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

11. Нажмите на кнопку **Готово**.

    Задача будет создана и отобразится в списке задач.

12. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

13. В окне свойств задачи укажите общие параметры задачи.

14. Нажмите на кнопку **Сохранить**.

15. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной деинсталляции выбранное приложение будет удалено с выбранных устройств.

Ограничения удаленной деинсталляции

Иногда удаленная деинсталляция приложений сторонних производителей может завершится предупреждением: "Удаление на этом устройстве завершено с предупреждениями: Приложение для деинсталляции не установлено". Эта проблема возникает, когда приложение для деинсталляции, уже было деинсталлировано или было установлено только для одного пользователя. Приложения, установленные для одного пользователя (далее также "приложения для каждого пользователя"), становятся невидимыми и не могут быть деинсталлированы удаленно, если пользователь не вошел в систему.

Такое поведение отличается от поведения приложений, предназначенных для использования несколькими пользователями на одном устройстве (далее также "приложения устройства"). Приложения для каждого устройства видны и доступны всем пользователям этого устройства.

Поэтому приложения для каждого пользователя должны быть деинсталлированы только когда пользователь вошел в систему.

Источники информации об установленных приложениях

Агент администрирования получает информацию о программном обеспечении, установленном на устройствах Windows, из следующих ключей реестра:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о приложениях, установленных для всех пользователей.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о приложениях, установленных для всех пользователей.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о приложениях, установленных для текущего пользователя.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о приложениях, установленных для набора пользователей.

Задачи

В этом разделе описаны задачи, которые используются в Kaspersky Security Center.

О задачах

Kaspersky Security Center управляет работой приложений безопасности "Лаборатории Касперского", установленных на устройствах, путем создания и запуска *задач*. С помощью задач выполняются установка, запуск и остановка приложений, проверка файлов, обновление баз и модулей приложений, другие действия с приложениями.

Вы можете создать задачу для приложения в Kaspersky Security Center Web Console, только если для этого приложения установлен плагин управления на Сервере Kaspersky Security Center Web Console.

Задачи могут выполняться на Сервере администрирования и на устройствах.

Задачи, которые выполняются на Сервере администрирования, включают:

- автоматическая рассылка отчетов;
- загрузку обновлений в хранилище;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных.

На устройствах выполняются следующие типы задач:

- *Локальные задачи* – это задачи, которые выполняются на конкретном устройстве.

  Локальные задачи могут быть изменены не только администратором средствами Консоли администрирования, но и пользователем удаленного устройства (например, в интерфейсе приложения безопасности). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором, как более приоритетные.

- *Групповые задачи* – это задачи, которые выполняются на всех устройствах указанной группы.

  Если иное не указано в свойствах задачи, групповая задача также распространяется на подгруппы указанной группы. Групповые задачи также действуют (опционально) и на устройства, подключенные к подчиненным и виртуальным Серверам администрирования, размещенным в этой группе и подгруппах.

- *Глобальные задачи* – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.

Для каждого приложения вы можете создавать любое количество групповых задач, глобальных задач и локальных задач.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

Запуск задач на устройстве выполняется только в том случае, если запущено приложение, для которого созданы эти задачи.

Результаты выполнения задач сохраняются в журнале событий операционной системы на каждом устройстве, в журнале событий на Сервере администрирования и в базе данных Сервера администрирования.

Не используйте в параметрах задач конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

Область задачи

Область применения задачи – это подмножество устройств, на которых выполняется задача. Существуют следующие типы областей задачи:

- Область *локальной задачи* – само устройство.
- Область *задачи Сервера администрирования* – Сервер администрирования.
- Область *групповой задачи* – перечень устройств, входящих в группу.

При создании *глобальной задачи* можно использовать следующие методы определения ее области:

- Вручную указать требуемые устройства.

  В качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал), 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

Чтобы создать задачу:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте шагам мастера.
3. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
4. Нажмите на кнопку **Готово**.

Задача будет создана и отобразится в списке задач.

Чтобы создать задачу, назначенную выбранным устройствам:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.

   Отобразится список управляемых устройств.
2. В списке управляемых устройств установите флажки рядом с устройствами, для которых нужно запустить задачу. Вы можете использовать функции поиска и фильтрации, чтобы найти необходимые устройства.
3. Нажмите на кнопку **Запустить задачу** и выберите **Создание задачи**.

   Запустится мастер создания задачи.

   На первом шаге мастера вы можете удалить устройства, выбранные для включения в область действия задачи. Следуйте инструкциям мастера.
4. Нажмите на кнопку **Готово**.

Задача создана для выбранных устройств.

Запуск задачи вручную

Приложение запускает задачи в соответствии с расписанием, заданным в свойствах каждой задачи. Вы можете запустить задачу вручную в любое время из списка задач. Также можно выбрать устройства в списке **Управляемые устройства** и запустить для них существующую задачу.

Чтобы запустить задачу вручную:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. В отобразившемся списке задач установите флажок напротив задачи, которую вы хотите запустить.
3. Нажмите на кнопку **Запустить**.

Задача будет запущена. Вы можете проверить статус задачи в столбце **Статус** или нажав на кнопку **Результат выполнения**.

Просмотр списка задач

Вы можете просмотреть список задач, созданных в Kaspersky Security Center.

Чтобы просмотреть список задач,

в главном окне приложения перейдите в раздел **Активы (Устройства)** → **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**.

Общие параметры задач

Этот раздел содержит описание параметров, которые вы можете просмотреть и настроить для большинства ваших задач. Список доступных параметров зависит от настраиваемой задачи.

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- Параметры перезагрузки операционной системы:

  - **Не перезагружать устройство**

    Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

  - **Перезагрузить устройство**

    В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

  - **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 расписания задачи:

  Типы расписаний могут изменяться в зависимости от задачи.

  - **Параметры Запуск задачи:**

    - **Каждый N час**

      Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

      По умолчанию задача запускается каждые 6 часов, начиная с текущих системной даты и времени.

    - **Каждые N дней**

      Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются приложением, для которого вы создаете задачу.

      По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

    - **Каждые N минут**

      Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

      По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

    - **По дням недели**

      Задача выполняется регулярно, в указанные дни недели, в указанное время.

      По умолчанию задача запускается каждую пятницу в 18:00:00.

    - **Ежемесячно**

      Задача выполняется регулярно, в указанный день месяца, в указанное время.

      В месяцах, у которых нет указанного дня, задача выполняется в последний день.

      По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

    - **Вручную**

      Задача не запускается автоматически. Вы можете запустить задачу только вручную.

      По умолчанию выбран этот вариант.

    - **Один раз**

      Задача выполняется один раз, в указанные дату и время (по умолчанию в день создания задачи).

- **Немедленно**

  Задача запускается сразу после сохранения ее параметров.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию указано время 18:00 и не выбраны дни месяца.

  > Обратите внимание, что вы выбираете порядковый номер дня недели в месяце, а не конкретную дату в месяце или номер недели (первая, вторая неделя месяца). Например, если вы выберите ячейку **Вт** в строке **Первая**, в этом случае задача будет запускаться каждый первый вторник каждого нового месяца.

  Вы можете выбрать несколько дней недели.

- **При загрузке обновлений в хранилище**

  Эта задача запускается после загрузки обновлений в хранилище. Например, вам может понадобиться это расписание для задачи поиска уязвимостей и требуемых обновлений.

- **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.

- Устройства, которым будет назначена задача:

  - **Выбрать устройства, обнаруженные в сети Сервером администрирования**

    В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

    Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

- **Задать адреса устройств вручную или импортировать из списка**

  Вы можете задавать 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.

- **Назначить задачу группе администрирования**

  Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

  Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

  Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, так как групповые задачи подчиняются параметрам групп безопасности, к которым они относятся.

- Параметры учетной записи:

  - **Учетная запись по умолчанию.**

    Задача будет запускаться под той же учетной записью, под которой было установлено и запущено приложение, выполняющее эту задачу.

    По умолчанию выбран этот вариант.

  - **Задать учетную запись**

    В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.

  - **Учетная запись.**

    Учетная запись, от имени которой будет запускаться задача.

  - **Пароль.**

    Пароль учетной записи, от имени которой будет запускаться задача.

Параметры, заданные после создания задачи

Вы можете задать следующие параметры только после создания задачи.

- Параметры групповой задачи:
  - **Распространить на подгруппы**

    Этот параметр доступен только в свойствах групповых задач.

    Когда этот параметр включен, область действия задачи включает в себя:
    - группу администрирования, которую вы выбрали при создании задачи;
    - группы администрирования, подчиненные по отношению к выбранной группе администрирования на любом уровне вниз по иерархии групп.

    Если этот параметр выключен, в состав задачи входит только та группа администрирования, которую выбрали при создании задачи.

    По умолчанию параметр включен.

  - **Распространить на подчиненные и виртуальные Серверы администрирования**

    При включении этого параметра задача, действующая на главном Сервере администрирования, применяется и на подчиненных Серверах администрирования (в том числе виртуальных). Если на подчиненном Сервере администрирования уже существует задача такого же типа, то на подчиненном Сервере администрирования применяются обе задачи – существующая и унаследованная от главного Сервера администрирования.

    Этот параметр доступен, только если параметр **Распространить на подгруппы** включен.

    По умолчанию параметр выключен.

- Дополнительные параметры расписания:
  - **Включать устройства перед запуском задачи функцией Wake-on-LAN за**

    Если флажок установлен, операционная система на устройстве будет загружаться за указанное время до начала выполнения задачи. Время, заданное по умолчанию, – 5 минут.

    Включите этот параметр, если вы хотите, чтобы задача выполнялась на всех клиентских устройствах из области задач, включая те устройства, которые выключены, когда задача вот-вот начнется.

    Если нужно, чтобы устройства автоматически выключались после выполнения задачи, включите параметр **Выключать устройства после выполнения задачи**. Параметр находится в этом же окне.

    По умолчанию параметр выключен.

  - **Выключать устройства после выполнения задачи**

    Например, вы можете включить этот параметр для задачи установки обновлений, которая устанавливает обновления на клиентские устройства каждую пятницу после рабочего времени, а затем выключает эти устройства на выходные.

    По умолчанию параметр выключен.

- **Остановить, если задача выполняется дольше**

  По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

  Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

  По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

- Параметры уведомления:

  - Блок **Сохранять информацию о результатах**:

    - **Хранить в базе данных Сервера администрирования в течение (сут)**

      События приложения, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся на Сервере администрирования в течение указанного количества дней. По истечении этого периода информация удаляется с Сервера администрирования.

      По умолчанию параметр включен.

    - **Хранить в журнале событий ОС на устройстве**

      События приложения, связанные с выполнением задачи, хранятся локально в журнале событий Windows каждого клиентского устройства.

      По умолчанию параметр выключен.

    - **Хранить в журнале событий ОС на Сервере администрирования**

      События приложения, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся централизованно в журнале событий Windows операционной системы Сервера администрирования.

      По умолчанию параметр выключен.

    - **Сохранять все события**

      Если выбран этот параметр, в журнал событий записываются все события, связанные с задачей.

    - **Сохранять события, связанные с ходом выполнения задачи**

      Если выбран этот параметр, в журнал событий записываются только события, связанные с выполнением задачи.

    - **Сохранять только результат выполнения задачи**

      Если выбран этот параметр, в журнал событий записываются только события, связанные с результатами выполнения задачи.

  - **Уведомлять администратора о результатах**

    Вы можете выбрать способы, с помощью которых администраторы получают уведомления о результатах выполнения задачи: по электронной почте, по SMS и при запуске исполняемого файла. Чтобы настроить параметры уведомления, перейдите по ссылке **Параметры**.

    По умолчанию отключены все способы уведомлений.

- **Уведомлять только об ошибках**

  Если этот параметр включен, администраторы получают уведомление, только если задача завершается с ошибкой.

  Если этот параметр выключен, администраторы получают уведомление после каждого завершения задачи.

  По умолчанию параметр включен.

- Параметры безопасности.
- Параметры области действия задачи.

  В зависимости от того, как определяется область действия задачи, присутствуют следующие параметры:

  - **Устройства**

    Если область действия задачи определяется группами администрирования, вы можете просмотреть эту группу. Никакие изменения здесь недоступны. Однако вы можете настроить **Исключения из области действия задачи**.

    Если область действия задачи определяется списком устройств, вы можете изменить этот список, добавив и удалив устройства.

  - **Выборка устройств**

    Вы можете изменить выборку устройств, к которым применяется задача.

  - **Исключения из области действия задачи**

    Вы можете указать группу устройств, к которым не применяется задача. Группы, подлежащие исключению, могут быть только подгруппами группы администрирования, к которой применяется задача.

- **История ревизий**.

Экспорт задачи

Kaspersky Security Center 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 **Активы (Устройства)** → **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 позволяет импортировать задачу из файла KLT. Файл KLT содержит экспортированную задачу и ее параметры.

Чтобы импортировать задачу:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **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)**.

Запуск мастера изменения паролей задач

Для не-локальной задачи, можно указать учетную запись, с правами которой будет запускаться задача. Учетную запись можно указать во время создания задачи или в свойствах существующей задачи. Если указанная учетная запись используется в соответствии с правилами безопасности, установленными в организации, эти правила могут требовать периодического изменения пароля учетной записи. После истечения срока действия пароля учетной записи и задания нового пароля, задача не будет запускаться до тех пор, пока вы не укажете новый действующий пароль в свойствах задачи.

Мастер изменения паролей задач позволяет автоматически заменить старый пароль на новый во всех задачах, в которых указана учетная запись. Вы также можете изменить пароль вручную в свойствах каждой задачи.

Чтобы запустить мастер изменения паролей задач

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.

2. Нажмите на кнопку **Управление учетными данными учетной записи для запуска задач**.

Следуйте далее указаниям мастера.

Шаг 1. Выбор учетных данных

Укажите новые учетные данные, действующие в вашей системе (например, в Active Directory). При переходе на следующий шаг мастера, Kaspersky Security Center проверяет, совпадает ли имя указанной учетной записи с именем учетной записи в свойствах каждой не-локальной задачи. Если имена учетных записей совпадают, пароль в свойствах задачи автоматически меняется на новый.

Чтобы указать новую учетную запись, выберите один из вариантов:

- **Использовать текущую учетную запись**

  Мастер использует имя учетной записи, под которой вы в настоящее время вошли в Kaspersky Security Center Web Console. Вручную укажите пароль учетной записи в поле **Актуальный пароль для использования в задачах**.

- **Указать другую учетную запись**

  Укажите имя учетной записи, под которой должны запускаться задачи. Укажите пароль учетной записи в поле **Актуальный пароль для использования в задачах**.

При заполнении поля **Предыдущий пароль (необязательно; если вы хотите заменить его на текущий)** Kaspersky Security Center заменит пароль только для тех задач, для которых совпадают значения имени и старого пароля. Замена выполняется автоматически. Во всех остальных случаях необходимо выбрать действие, выполняемое на следующем шаге мастера.

Шаг 2. Выбор выполняемого действия

Если на первом шаге мастера вы не указали предыдущий пароль или указанный старый пароль не соответствует паролям, которые указаны в свойствах задач, необходимо выбрать действие, выполняемое с этими задачами.

Чтобы выбрать действие с задачей:

1. Установите флажок около задачи, с которой вы хотите выполнить действие.
2. Выполните одно из следующих действий:

   - Чтобы удалить пароль в свойствах задачи, нажмите **Удалить учетные данные**.

     Задача переключена на запуск под учетной записью по умолчанию.

   - Чтобы заменить пароль на новый, нажмите **Принудительно изменить пароль, даже если старый пароль неверен или не указан**.

   - Чтобы отменить изменение пароля, нажмите **Действие не выбрано**.

   Выбранные действия применяются после перехода к следующему шагу мастера.

Шаг 3. Просмотр результатов

На последнем шаге мастера просмотрите результаты для каждой из обнаруженных задач. Для завершения работы мастера нажмите на кнопку **Готово**.

Создание задачи Удаленное выполнение скриптов

Вы можете создать задачу *Удаленное выполнение скриптов* для выполнения инсталляционного пакета на клиентском устройстве и удаленной установки приложения.

Инсталляционный пакет содержит ZIP-архив с набором скриптов для выполнения на клиентских устройствах, а также файл manifest.json. Подробнее о создании этого типа инсталляционного пакета см. статью.

Эту задачу нужно запускать только на устройствах с Агентом администрирования для Linux.

Чтобы запустить задачу Удаленное выполнение скриптов:

1. Перейдите в **Мастер создания задачи** и выберите тип задачи **Удаленное выполнение скриптов**.
2. Введите название задачи и выберите устройства, которым будет назначена задача. Нажмите на кнопку **Далее**.
3. Выберите инсталляционный пакет на основе ZIP-архива с файлом manifest.json для удаленного выполнения.

   Если вы не хотите повторно запускать задачу на устройствах, на которых она уже была выполнена, включите параметр **Не запускать эту задачу на устройствах, на которых она уже была выполнена**.
4. Выберите учетную запись для запуска задачи.

   Если вы выберете учетную запись по умолчанию, то задачу будет выполнять Агент администрирования (учетная запись root).

   При запуске задачи *Удаленное выполнение скриптов* вы не можете изменить учетную запись, которая назначена задаче. Чтобы изменить учетную запись, которой назначена задача, остановите задачу в параметрах задачи и создайте задачу снова с требуемой учетной записью.
5. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
6. Нажмите на кнопку **Готово**.

   Задача *Удаленное выполнение скриптов* создана и отображается в списке задач.

После получения данных из задачи *Удаленное выполнение скриптов*, Агент администрирования ограничивает доступ к полученным данным для всех пользователей, кроме администратора и пользователя, указанного в параметрах задачи.

Удаленная установка приложений на устройства с помощью задачи Удаленное выполнение скриптов

Задачу *Удаленное выполнение скриптов* можно использовать для удаленной установки приложения на клиентское устройство с помощью создания пользовательского инсталляционного пакета.

О том, как подготовить архив для этой задачи, см. статью.

Чтобы создать инсталляционный пакет для удаленной установки приложения на клиентское устройство, в архив, который вы хотите загрузить для этой задачи, должны быть включены следующие файлы:

- `<имя пакета>.deb`
- **install.sh**

  ```
  sudo apt-get install <имя пакета>.deb
  ```

- **manifest.json**

  Схема JSON для удаленной установки приложения

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "install.sh",
      "args": "< введите аргументы, если необходимо >",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

  Описание массивов

  1. `version` – версия файла манифеста и задачи.

     В настоящее время единственное допустимое значение – 1.

  2. Элементы массива `actions` определяют состав и порядок выполнения скриптов в задаче.

     Порядок выполнения скрипта соответствует индексу (положению) элемента в массиве.

  3. Для каждого элемента массива `actions` определены следующие элементы.

     a. `type` – тип исполняемой команды из скриптов. В настоящее время значение всегда `execute`.

     b. `path` – путь к файлу скрипта в архиве.

     c. `args` – аргументы, которые передаются скрипту как часть исполняемой команды.

     d. `results` – массив, определяющий дальнейшие действия в зависимости от результата выполнения задачи.

        1. `code` – значение, возвращающее скрипт.

        2. `next` – действие, которое будет выполнено следующим. Действие `continue` переходит к выполнению следующего скрипта (элемента в массиве `actions`). Действие `break` останавливает задачу.

     e. `default_next` – действие, если скрипт возвращает значение, которого нет в `results`.

При запуске задачи *Удаленное выполнение скриптов* Агент администрирования загрузит инсталляционный пакет с приложением на клиентское устройство. Когда клиентское устройство получает инсталляционный пакет, Агент администрирования на этом устройстве анализирует файл manifest.json и определяет порядок выполнения скриптов и действий в зависимости от результата, а затем начинает выполнение.

После завершения задачи *Удаленное выполнение скриптов* приложение будет установлено на клиентском устройстве.

Настройка уведомлений и мониторинга для задачи Удаленное выполнение скриптов

Вы можете настроить мониторинг, поведение при сохранении событий и уведомления для задачи *Удаленное выполнение скриптов*.

Чтобы просмотреть статус задачи Удаленное выполнение скриптов:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.

   Отобразится список задач.

2. Выберите задачу и нажмите на **История устройства**.

   Отображается ход выполнения задачи.

Чтобы настроить поведение при сохранении событий:

1. В списке задач нажмите на название задачи и перейдите на вкладку **Параметры**.
2. В разделе **Уведомления** нажмите на кнопку **Параметры**.
3. Выберите один из следующих вариантов поведения приложения после выполнения задачи:

   - **Сохранять все события**.
   - **Сохранять события, связанные с ходом выполнения задачи**.
   - **Сохранять только результат выполнения задачи**.

     События сохраняются в разделе **История устройства** и **Хранилище событий**.

     По умолчанию сохраняются только результаты выполнения задачи.

     > Если вы выберете **Сохранять все события**, сохраняются только результаты выполнения задачи.

4. Если вы хотите сохранить события в базе данных Сервера администрирования, в журнале событий на Сервере администрирования или на устройстве, включите соответствующий параметр.

Подробнее о настройке уведомлений см. в этой статье.

Подготовка архива для задачи Удаленное выполнение скриптов

Архив для задачи *Удаленное выполнение скриптов* на основе файла manifest.json должен соответствовать следующим требованиям:

- Формат архива: ZIP.
- Общий размер: не более 1 ГБ.
- Количество файлов и папок в архиве не ограничено.

- Манифест-файл архива должен соответствовать приведенной ниже схеме и называться manifest.json. Схема проверяется только во время выполнения задачи на устройстве.

  Схема JSON манифест-файла и описание массивов

  Схема JSON

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
                    },
                    "path": {
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
                    "results":{
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
                                },
                                "next":{
                                    "type": "string",
                                    "enum": ["break", "continue"]
                                }
                            },
                            "required": [
                                "code",
                                "next"
                            ]
                        }
                    },
                    "default_next":{
                        "type": "string",
                        "enum": ["break", "continue"]
                    }
                },
```

```
                "required": [
                    "type",
                    "path",
                    "default_next"
                ]
            }
        }
    },
    "required": [
        "version",
        "actions"
    ]
}
```

Пример манифест-файла

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- Архив должен иметь следующую структуру:

```
manifest.json
<file1>
<file2>
<folder1>/<file3>
<folder2>/<folder3>/<file4>
...
<fileX>
```

`manifest.json` – это манифест-файл задачи.

`<file1>`, ..., `<fileX>` – это набор файлов со скриптами, которые нужно выполнить.

Создание инсталляционного пакета на основе манифест-файла

Чтобы создать инсталляционный пакета на основе манифест-файла:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
   - В главном окне приложения перейдите в раздел **Операции** → **Хранилища** → **Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Выберите параметр **Создать инсталляционный пакет для задачи "Удаленное выполнение скриптов" на основе архива ZIP с файлом manifest.json**.

4. Укажите имя инсталляционного пакета и нажмите на кнопку **Обзор**.

   Откроется стандартное окно Windows **Открыть**, в котором можно выбрать файл для создания инсталляционного пакета.

5. Выберите архивный файл, расположенный на доступных дисках. О том, как подготовить архив для этой задачи, см. статью.

   Файл начнет загружаться на Сервер администрирования Kaspersky Security Center.

   Начнется процесс создания инсталляционного пакета.

   В окне мастера отобразится информация о завершении процесса.

   Если инсталляционный пакет не создан, отобразится соответствующее сообщение.

6. Нажмите на кнопку **Готово**, чтобы закрыть окно мастера.

Созданный инсталляционный пакет загружается во вложенную папку Packages общей папки Сервера администрирования. После загрузки инсталляционный пакет появится в списке инсталляционных пакетов.

В списке инсталляционных пакетов доступных на Сервере администрирования, нажав на имя инсталляционного пакета, вы можете:

- Просмотреть следующие свойства инсталляционного пакета:
  - **Имя.** Название инсталляционного пакета.
  - **Источник.** Имя поставщика приложения.
  - **Версия.** Версия приложения.
  - **Создано.** Дата создания инсталляционного пакета.
  - **Изменено.** Дата изменения инсталляционного пакета.
  - **Путь.** Путь к пользовательскому инсталляционному пакету на Сервере администрирования.
- Изменить имя пакета и параметры командной строки. Эта функция доступна только для пакетов, которые не созданы на основе приложений "Лаборатории Касперского".

Управление клиентскими устройствами

Kaspersky Security Center 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 **Активы (Устройства)** → **Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием нужного устройства.

Откроется окно свойств выбранного устройства.

В верхней части окна свойств отображаются следующие вкладки, на которых представлены основные группы параметров:

- **Общие**

  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.

- **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:

  - **Операционная система**

  - **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.

- **Приложения**

  На этой вкладке отображается список приложений "Лаборатории Касперского", установленных на клиентском устройстве. На этой вкладке находятся кнопки **Запустить** и **Остановить**, которые позволяют запускать и останавливать выбранное приложение "Лаборатории Касперского" (кроме Агента администрирования). Вы можете использовать эти кнопки, если на управляемых устройствах доступен порт 15000 UDP для приема запросов на связь с Сервером администрирования. Если управляемое устройство недоступно для push-уведомлений, но включен режим постоянного подключения к Серверу администрирования (параметр **Не разрывать соединение с Сервером администрирования** в разделе **Общие** включен), кнопки **Запустить** и **Остановить** активны. Иначе при попытке запустить или остановить приложение появится сообщение об ошибке. Также вы можете нажать на имя приложения, чтобы просмотреть общую информацию о приложении, список событий, произошедших на устройстве, и параметры приложения.

- **Действующие политики и профили политик**

  На этой вкладке отображаются списки политик и профилей политик, которые назначены управляемому устройству.

- **Задачи**

  На вкладке **Задачи** вы можете управлять задачами клиентского устройства: просматривать список существующих задач, создавать новые, удалять, запускать и останавливать задачи, изменять их параметры и просматривать результаты выполнения. Список задач предоставляется на основании данных, полученных в ходе последней синхронизации клиента с Сервером администрирования. Информация о статусе задач запрашивается Сервером администрирования с клиентского устройства. Если на управляемых устройствах доступен порт 15000 UDP для приема запросов на связь с Сервером администрирования, отображается статус задачи и кнопки управления задачей активны. Если push-сервер не может получить доступ к управляемому устройству, но включен режим постоянного подключения к Серверу администрирования (параметр **Не разрывать соединение с Сервером администрирования** с Сервером администрирования в разделе **Общие** включен), действия с задачами доступны.

  В случае отсутствия связи статус не отображается и кнопки неактивны.

- **События**

  На вкладке **События** отображаются события, зарегистрированные на Сервере администрирования для выбранного клиентского устройства.

  Вы можете экспортировать, копировать и удалять события устройства.

- **Проблемы безопасности**

  На вкладке **Проблемы безопасности** можно просматривать, изменять и создавать проблемы безопасности для клиентского устройства. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором. Например, если пользователь постоянно переносит на устройство вредоносные приложения с личного съемного диска, администратор может создать проблему безопасности. Администратор может указать краткое описание случая и рекомендуемых действий (таких как дисциплинарные действия), которые должны быть предприняты против пользователя в тексте проблемы безопасности, и может добавить ссылку на пользователя или пользователей.

  Проблема безопасности, для которой выполнены необходимые действия, называется *обработанным*. Наличие необработанных проблем безопасности может быть выбрано условием для изменения статуса устройства на *Критический* или *Предупреждение*.

В разделе содержится список проблем безопасности, созданных для устройства. Проблемы безопасности классифицируются по уровню важности и типу. Тип проблемы безопасности определяется приложением "Лаборатории Касперского", которое создает проблему безопасности. Обработанные проблемы безопасности можно отметить в списке, установив флажок в столбце **Обработана**.

- **Теги**

  На вкладке **Теги** можно управлять списком ключевых слов, на основании которых выполняется поиск клиентского устройства: просматривать список существующих тегов, назначать теги из списка, настраивать правила автоматического назначения тегов, добавлять новые теги и переименовывать старые теги, удалять теги.

- **Дополнительно**

  Эта вкладка содержит следующие разделы:

  - **Реестр приложений**. В этом разделе можно просмотреть реестр установленных на клиентском устройстве приложений и обновлений для них, а также настроить отображение реестра приложений.

    Информация об установленных приложениях предоставляется в том случае, если установленный на клиентском устройстве Агент администрирования передает необходимую информацию на Сервер администрирования. Параметры передачи информации на Сервер администрирования можно настроить в окне свойств Агента администрирования или его политики в разделе **Хранилища**.

    При нажатии на имя приложения открывается окно, содержащее сведения о приложении и список пакетов обновлений, установленных для этого приложения.

  - **Исполняемые файлы**. В этом разделе отображаются исполняемые файлы, обнаруженные на клиентском устройстве.

  - **Точки распространения**. В этом разделе представлен список точек распространения, с которыми взаимодействует устройство.

    - **Экспортировать в файл**

      По кнопке **Экспортировать в файл** вы можете сохранить в файл список точек распространения, с которыми взаимодействует устройство. По умолчанию приложение экспортирует список устройств в файл формата CSV.

    - **Свойства**

      По кнопке **Свойства** вы можете посмотреть и настроить параметры точки распространения, с которым взаимодействует устройство.

  - **Реестр оборудования**. В этом разделе можно просмотреть информацию об оборудовании, установленном на клиентском устройстве.

    Если Агент администрирования установлен на устройстве с операционной системой Windows, он отправляет на Сервер администрирования следующую информацию об аппаратном обеспечении устройства:

    - оперативная память;
    - запоминающие устройства;
    - материнская плата;
    - процессор;

- сетевой адаптер;
- мониторы;
- видеоадаптер;
- звуковая плата.

Если Агент администрирования установлен на устройстве с операционной системой Linux или macOS, он отправляет на Сервер администрирования следующую информацию об аппаратном обеспечении устройства, если эта информация предоставляется операционной системой:

- общий объем оперативной памяти;
- общий объем запоминающих устройств;
- материнская плата;
- процессор;
- сетевой адаптер.

- **Применимые обновления**. В этом разделе можно просмотреть список обнаруженных на устройстве обновлений программного обеспечения, которые не были установлены.

- **Уязвимости в приложениях**. В этом разделе можно просмотреть список с информацией об уязвимостях сторонних приложений, установленных на клиентских устройствах.

  Чтобы сохранить уязвимости в файл, установите флажки рядом с уязвимостями, которые вы хотите сохранить, и нажмите на кнопку **Экспортировать в CSV** или на кнопку **Экспортировать в TXT**.

  Раздел содержит следующие параметры:

  - **Показывать только те уязвимости, которые можно закрыть**

    Если параметр включен, в разделе отображаются уязвимости, которые можно закрыть патчем.

    Если параметр выключен, в разделе отображаются и уязвимости, которые можно закрыть патчем, и уязвимости, для которых патч отсутствует.

    По умолчанию параметр включен.

  - **Свойства уязвимости**

    Нажмите на имя уязвимости в приложениях в списке, чтобы просмотреть свойства выбранной уязвимости в приложениях в отдельном окне. В окне свойств можно выполнить следующие действия:

    - Пропустить уязвимость в приложениях на этом управляемом устройстве (в Консоли администрирования или в Kaspersky Security Center Web Console).
    - Просмотреть список рекомендуемых исправлений для уязвимости.
    - Вручную указать обновления программного обеспечения для закрытия уязвимости (в Консоли администрирования или в Kaspersky Security Center Web Console).
    - Просмотреть экземпляр уязвимости.
    - Просмотреть список существующих задач для закрытия уязвимости и создать задачи для закрытия уязвимости.

- **Удаленная диагностика**. В этом разделе можно выполнять удаленную диагностику клиентских устройств.

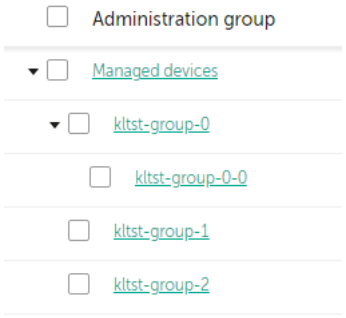
Если вы используете СУБД PostgreSQL, MariaDB или MySQL, на вкладке **События** может отображаться неполный список событий для выбранного клиентского устройства. Это происходит, когда СУБД хранит очень большое количество событий. Вы можете увеличить количество отображаемых событий, выполнив одно из следующих действий:

- Удалить ненужные события.
- Сократить срок хранения ненужных событий.

Чтобы увидеть полный список событий, зарегистрированных на Сервере администрирования для устройства, используйте Отчеты.

Создание групп администрирования

Сразу после установки Kaspersky Security Center в иерархии групп администрирования присутствует только одна группа администрирования – **Управляемые устройства**. При создании иерархии групп администрирования в состав папки **Управляемые устройства** можно включать устройства и виртуальные машины и добавлять вложенные группы (см. рисунок ниже).



Просмотр иерархии групп администрирования

Чтобы создать группу администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Иерархия групп**.
2. В структуре группы администрирования выберите группу администрирования, в состав которой должна входить новая группа администрирования.
3. Нажмите на кнопку **Добавить**.
4. В открывшемся окне **Имя новой группы администрирования** введите имя группы и нажмите на кнопку **Добавить**.

   В результате в иерархии групп администрирования появится новая группа администрирования с заданным именем.

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 **Активы (Устройства)** → **Иерархия групп**.
2. Нажмите на кнопку **Импортировать**.

   В результате запускается мастер создания структуры групп администрирования. Следуйте далее указаниям мастера.

Добавление устройств в состав группы администрирования вручную

Вы можете перемещать устройства в группы администрирования автоматически, создавая правила перемещения устройств, или вручную, перемещая устройства из одной группы администрирования в другую, или добавляя устройства в выбранную группу администрирования. В этом разделе описано, как вручную добавить устройства в группу администрирования.

Чтобы вручную добавить одно или несколько устройств в состав выбранной группы администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. Перейдите по ссылке **Текущий путь:** `<текущий_путь>` над списком.
3. В открывшемся окне выберите группу администрирования, в которую требуется добавить устройства.
4. Нажмите на кнопку **Добавить устройства**.

   В результате запустится мастер перемещения устройств.
5. Составьте список устройств, которые вы хотите добавить в группу администрирования.

   > В список устройств могут быть добавлены только те устройства, информация о которых уже была добавлена в базу данных Сервера администрирования при подключении устройства или в результате обнаружения устройств.

   Выберите, как вы хотите добавить устройства в список:

   - Нажмите на кнопку **Добавить устройства** и укажите устройства одним из следующих способов:
     - Выберите устройства из списка устройств, обнаруженных Сервером администрирования.
     - Укажите IP-адреса устройств или IP-диапазон.

       > 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, 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, а также следующие запрещенные символы: \ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %

6. Просмотрите список устройств, которые будут добавлены в группу администрирования. Вы можете редактировать список, добавляя или удаляя устройства.

7. После того как вы убедитесь, что в списке нет ошибок, нажмите на кнопку **Далее**.

Мастер обрабатывает список устройств и отображает результат. После завершения работы мастера выбранные устройства включаются в состав группы администрирования и отображаются в списке устройств под именами, установленными для них Сервером администрирования.

Перемещение устройств или кластеров в состав группы администрирования вручную

Устройства можно перемещать из одной группы администрирования в другую или из группы нераспределенных устройств в группу администрирования.

Также можно перемещать кластеры или массивы серверов из одной группы администрирования в другую. При перемещении кластера или массива серверов в другую группу, все его узлы перемещаются вместе с ним, так как кластер и любой из его узлов всегда принадлежат к одной группе администрирования. При выборе одного узла кластера на вкладке **Устройства**, кнопка **Переместить в группу** становится недоступной.

Чтобы переместить одно или несколько устройств или кластеров в состав выбранной группы администрирования:

1. Откройте группу администрирования, в которую вы хотите переместить устройства. Для этого выполните одно из следующих действий:

   - Чтобы открыть группу администрирования, в главном меню перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**, перейдите по ссылке в поле **Текущий путь** и в открывшейся слева панели выберите группу администрирования.

   - Чтобы открыть группу **Нераспределенные устройства**, в главном меню перейдите в раздел **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.

2. Если группа администрирования содержит кластеры или массивы серверов, раздел **Управляемые устройства** разделен на две вкладки – **Устройства** и **Кластеры и массивы серверов**. Откройте вкладку объекта, который хотите переместить.

3. Установите флажки рядом с устройствами или кластерами, которые требуется переместить в другую группу.

4. Нажмите на кнопку **Переместить в группу**.

5. В иерархии групп администрирования установите флажок рядом с группой администрирования, в которую вы хотите переместить выбранные устройства или кластеры.

6. Нажмите на кнопку **Переместить**.

Выбранные устройства или кластеры перемещаются в выбранную группу администрирования.

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 **Активы (Устройства)** → **Правила перемещения**.

2. Нажмите на кнопку **Добавить**.

3. В открывшемся окне укажите следующие данные на вкладке **Общие**:

   - **Имя правила**

     Укажите имя нового правила активации.

     Если вы копируете правило, новое правило получает такое же имя, как и исходное правило, но к нему добавляется индекс в скобках, например: (1).

   - **Группа администрирования**

     Выберите группу администрирования, в которую будут автоматически перемещаться устройства.

   - **Активное правило**

     Если этот параметр включен, правило включено и начинает применяться сразу после сохранения.

     Если этот параметр выключен, правило создается, но оно не включено. Правило не будет работать до тех пор, пока вы не включите этот параметр.

   - **Перемещать только устройства, 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 повысить или понизить приоритет правила перемещения, с помощью мыши переместите правило вверх или вниз по списку соответственно.

Если выбран параметр **Применять правило постоянно**, правило перемещения применяется независимо от приоритета. Такие правила применяются по расписанию, которое Сервер администрирования устанавливает автоматически.

Если атрибуты устройства удовлетворяют сразу нескольким правилам, то устройство будет перемещено в целевую группу того правила, которое имеет больший приоритет (стоит в списке правил выше).

Копирование правил перемещения устройств

Можно копировать правила перемещения устройств, например, если требуется несколько одинаковых правил для разных целевых групп администрирования.

Чтобы скопировать правило перемещения устройств:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Правила перемещения**.
   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Правила перемещения**.

   Отобразится список правил перемещения устройств.

2. Установите флажок напротив правила, которое требуется скопировать.

3. Нажмите на кнопку **Копировать**.

4. В открывшемся окне при необходимости измените данные на вкладке **Общие** либо оставьте существующие значения, если требуется только скопировать правило, без изменения параметров:

   - **Имя правила**

     Укажите имя нового правила активации.

     Если вы копируете правило, новое правило получает такое же имя, как и исходное правило, но к нему добавляется индекс в скобках, например: (1).

- **Группа администрирования**

  Выберите группу администрирования, в которую будут автоматически перемещаться устройства.

- **Активное правило**

  Если этот параметр включен, правило включено и начинает применяться сразу после сохранения.

  Если этот параметр выключен, правило создается, но оно не включено. Правило не будет работать до тех пор, пока вы не включите этот параметр.

- **Перемещать только устройства, 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, 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 15.1** или **Сервер администрирования Kaspersky Security Center 15.1**.

  Если вы не выберете управляемое приложение, условие не будет применяться.

- **Версия операционной системы**

  Можно выбирать клиентские устройства на основе версии операционной системы. Для этого укажите операционные системы, которые должны быть установлены на клиентских устройствах. В результате правило перемещения устройств применяется к клиентским устройствам с выбранными операционными системами.

  Если этот параметр выключен, условие не применяется. По умолчанию параметр выключен.

- **Архитектура операционной системы**

  Можно выбирать клиентские устройства по разрядности операционной системы. В поле **Архитектура операционной системы** можно выбрать одно из следующих значений:

  - **Нет данных**
  - **x86**
  - **AMD64**
  - **IA64**

  Чтобы проверить какая архитектура используется в операционной системе клиентских устройств:

  1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
  2. Нажмите на кнопку **Параметры столбцов** справа (⚙).
  3. Выберите параметр **Архитектура операционной системы** и нажмите на кнопку **Сохранить**.

     После этого для каждого управляемого устройства отобразится архитектура операционной системы.

- **Версия пакета обновления операционной системы**

  В поле можно указать версию пакета установленной операционной системы (в формате *X.Y*), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

- **Пользовательский сертификат**

  Выберите одно из следующих значений:

  - **Установлено**. Правило перемещения устройств применяется только к мобильным устройствам с мобильным сертификатом.
  - **Не установлена**. Правило перемещения устройств применяется только к мобильным устройствам без мобильного сертификата.
  - **Значение не выбрано**. Условие не применяется.

- **Номер сборки операционной системы**

  > Этот параметр применим только для операционных систем Windows.

  Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить правило перемещения устройств для всех номеров сборки, кроме указанного.

- **Номер выпуска операционной системы**

  > Этот параметр применим только для операционных систем Windows.

  Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить правило перемещения устройств для всех номеров сборки, кроме указанного.

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 домена, указанного в списке под параметром.

  По умолчанию параметр выключен.

- **Включать дочерние подразделения**

  Если этот параметр включен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы домена.

  По умолчанию параметр выключен.

- **Перемещать устройства из дочерних подразделений в соответствующие подгруппы**
- **Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств**
- **Удалять подгруппы, отсутствующие в домене**
- **Устройство включено в следующую группу безопасности домена**

  Если этот параметр включен, правило перемещения устройств применяется к устройствам из доменной группы безопасности, указанной в списке под параметром.

  По умолчанию параметр выключен.

Вкладка Облачные сегменты

На этой вкладке 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.

О кластерах и массивах серверов

Kaspersky Security Center поддерживает кластерную технологию. Если Агент администрирования передает Серверу администрирования информацию о том, что приложение, установленное на клиентском устройстве, является частью массива сервера, то клиентское устройство становится узлом кластера.

Если группа администрирования содержит кластеры или массивы серверов, на странице **Управляемые устройства** отображаются две вкладки: одна для отдельных устройств, другая для кластеров и массивов серверов. После обнаружения управляемых устройств в качестве узлов кластера, кластер добавляется как отдельный объект на вкладку **Кластеры и массивы серверов**.

Узлы кластера или массивы серверов перечислены на вкладке **Устройства** вместе с другими управляемыми устройствами. Вы можете просматривать свойства узлов как отдельных устройств и выполнять другие операции, но удалить узел кластера или переместить его в другую группу администрирования отдельно от его кластера 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 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 **Активы (Устройства)** → **Управляемые устройства** → **Кластеры и массивы серверов**.

   Отображается список кластеров и массивов серверов.

2. Нажмите на имя нужного кластера или массива серверов.

Откроется окно свойств выбранного кластера или массива серверов.

Общие

Раздел **Общие** отображает общую информацию о кластере или массиве серверов. Информация предоставляется на основании данных, полученных в ходе последней синхронизации узлов кластера с Сервером администрирования:

Имя

Описание

Windows-домен

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 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.

Просмотр и настройка действий, когда устройство неактивно

Если клиентские устройства группы администрирования неактивны, вы можете получать уведомления об этом. Вы также можете автоматически удалять такие устройства.

Чтобы просмотреть или настроить действия, когда устройства неактивны в группе администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Иерархия групп**.
2. Выберите имя требуемой группы администрирования.

   Откроется окно свойств группы администрирования.
3. В окне свойств 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 присваивает статус каждому управляемому устройству. Конкретный статус зависит от того, выполнены ли условия, определенные пользователем. В некоторых случаях при присваивании статуса устройству Kaspersky Security Center учитывает видимость устройства в сети (см. таблицу ниже). Например, если управляемому устройству был присвоен статус *Критический*, так как выполнено условие *Базы устарели*, а затем для устройства стало видимо в сети, то устройству присваивается статус *OK*. Если Kaspersky Security Center не находит устройство в сети в течение двух часов, видимость устройства принимает значение *Не в сети*.

Существуют следующие статусы:

- *Критический* или *Критический / Видим в сети*.
- *Предупреждение* или *Предупреждение / Видим в сети*.
- *OK* или *OK / Видим в сети*.

В таблице ниже приведены условия по умолчанию для присвоения устройству статуса *Критический* или *Предупреждение* и их возможные значения.

Условия присвоения статусов устройству

Условие	Описание условия	Доступные значения
Приложение безопасности не установлено	Агент администрирования установлен на устройстве, но не установлено приложение безопасности.	• Переключатель включен. • Переключатель выключен.
Обнаружено много вирусов	В результате работы задач поиска вирусов, например, задачи *Поиск вредоносного ПО*, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение.	Более 0.
Уровень постоянной защиты отличается от уровня, установленного администратором	Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства.	• Остановлена. • Приостановлена. • Выполняется.
Давно не выполнялся поиск вредоносного ПО	Устройство видимо в сети и на устройстве установлено приложение безопасности, но ни задача *Поиск вредоносного ПО*, ни задача локальной проверки не выполнялись больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее.	Более 1 дня.
Базы устарели	Устройство видимо в сети и на устройстве установлено приложение безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее.	Более 1 дня.

Условие	Описание условия	Доступные значения
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. Управляемые устройства могут иметь статус, определяемый управляемыми приложениями, независимо от параметров Kaspersky Security Center. После того как этот статус вернет один из статусов, определенных Kaspersky Security Center, Сервер администрирования Kaspersky Security Center присваивает управляемому устройству предельный статус из тех, которые были возвращены управляемым приложением и присвоены Сервером администрирования Kaspersky Security Center. Статусы устройств определенные приложениями имеют описания, переданные управляемыми приложениями. Вы можете просмотреть описания в списке управляемых устройств в столбце **Описание статуса**.	• Переключатель выключен. • Переключатель включен.
На устройстве заканчивается дисковое пространство	Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы *Критический* или *Предупреждение* меняются на статус *OK*, когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению.	Более чем 0 МБ.
Устройство стало неуправляемым	Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования.	• Переключатель выключен. • Переключатель включен.
Защита выключена	Устройство видимо в сети, но приложение безопасности на устройстве отключено больше указанного времени. В этом случае состояние приложения безопасности *Остановлено* или *Сбой* и отличается от следующих: *Запускается*, *Выполняется* или *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 позволяет настроить автоматическое переключение статуса устройства в группе администрирования при выполнении заданных условий. При выполнении заданных условий клиентскому устройству присваивается один из статусов: *Критический* или *Предупреждение*. При невыполнении заданных условий клиентскому устройству присваивается статус *OK*.

Разным значениям одного условия могут соответствовать разные статусы. Например, по умолчанию при соблюдении условия **Базы устарели** со значением **Более 3 дней** клиентскому устройству присваивается статус *Предупреждение*, а со значением **Более 7 дней** – статус *Критический*.

Если вы обновляете Kaspersky Security Center с предыдущей версии, значение условия **Базы устарели** для назначения статуса *Критический* или *Предупреждение* не изменится.

Настройка переключения статусов устройств

Вы можете изменить условия присвоения статусов *Критический* или *Предупреждение* устройству.

Чтобы изменить статус устройства на Критический:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Иерархия групп**.
2. В открывшемся списке групп перейдите по ссылке с названием группы, для которой вы хотите изменить переключение статусов устройств.
3. В 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 **Активы (Устройства)** → **Иерархия групп**.
2. В открывшемся списке групп перейдите по ссылке с названием группы, для которой вы хотите изменить переключение статусов устройств.
3. В 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*.

Удаленное подключение к рабочему столу клиентского устройства

Администратор может 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 администратор получает 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 рабочей станции администратора. Вы используете эту утилиту для туннелирования соединения между клиентским устройством и Сервером администрирования.

  Kaspersky Security Center 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. После подключения администратора к сеансу пользователь устройства будет отключен от сеанса без предварительного уведомления.

Чтобы удалено подключиться к рабочему столу клиентского устройства:

1. В Консоли администрирования на основе MMC в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
2. В открывшемся окне свойств Сервера администрирования перейдите в раздел **Параметры подключения к Серверу администрирования → Порты подключения**.
3. Убедитесь, что параметр **Открыть RDP-порт для Kaspersky Security Center Web Console** включен.
4. В Kaspersky Security Center Web Console перейдите в раздел **Активы (Устройства) → Управляемые устройства**.
5. В поле **Текущий путь** над списком управляемых устройств перейдите по ссылке.
6. В открывшейся панели слева выберите группу администрирования, содержащую устройство, к которому вы хотите получить доступ.
7. Установите флажок напротив устройства, к которому вы хотите получить доступ.
8. Нажмите на кнопку **Подключиться к удаленному рабочему столу**.

   Откроется окно Удаленный рабочий стол (только Windows).
9. Включите параметр **Разрешить подключение к удаленному рабочему столу на управляемом устройстве**. В этом случае соединение будет установлено, даже если удаленные подключения в настоящее время запрещены в параметрах операционной системы на управляемом устройстве.

   Этот параметр доступен только при наличии лицензии на Системное администрирование.
10. Нажмите на кнопку **Загрузить**, чтобы загрузить утилиту klsctunnel.
11. 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 Удаленный рабочий стол (только Windows), чтобы сгенерировать новый объект BLOB.

12. Запустите утилиту klsctunnel.

    Откроется окно утилиты.

13. Вставьте скопированный текст в текстовое поле.

14. Если вы используете прокси-сервер, установите флажок **Использовать прокси-сервер**, а затем укажите параметры подключения к прокси-серверу.

15. Нажмите на кнопку **Открыть порт**.

    Откроется окно входа в систему подключения к удаленному рабочему столу.

16. Укажите учетные данные учетной записи, под которой вы в настоящий момент входите Kaspersky Security Center Web Console.

17. 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

Администратор может 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.

Администратор может подключиться к существующему сеансу на клиентском устройстве без отключения пользователя, работающего в этом сеансе. В этом случае у администратора и 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 рабочей станции администратора. Вы используете эту утилиту для туннелирования соединения между клиентским устройством и Сервером администрирования.

  Kaspersky Security Center 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 запрос от администратора на подключение. Информация о процессе удаленной работы с устройством и результатах этой работы не сохраняется в отчетах Kaspersky Security Center.

  Администратор может настроить аудит действий на удаленном клиентском устройстве. В ходе аудита приложение сохраняет информацию о файлах на клиентском устройстве, которые открывал и/или изменял администратор.

Для подключения к рабочему столу клиентского устройства с помощью совместного доступа к рабочему столу Windows требуется выполнение следующих условий:

- На рабочем месте администратора установлена операционная система Microsoft Windows Vista или более поздняя версия. Тип операционной системы устройства, на котором установлен Сервер администрирования, не является ограничением для подключения с помощью совместного доступа к рабочему столу Windows.

  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 реестре Windows.

- На клиентском устройстве установлена операционная система Microsoft Windows Vista или более поздняя версия.

- Kaspersky Security Center использует лицензию на Системное администрирование.

Чтобы подключиться к рабочему столу клиентского устройства с помощью совместного доступа к рабочему столу Windows:

1. В Консоли администрирования на основе MMC в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
2. В открывшемся окне свойств Сервера администрирования перейдите в раздел **Параметры подключения к Серверу администрирования** → **Порты подключения**.
3. Убедитесь, что параметр **Открыть RDP-порт для Kaspersky Security Center Web Console** включен.
4. В Kaspersky Security Center Web Console перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
5. В поле **Текущий путь** над списком управляемых устройств перейдите по ссылке.
6. В открывшейся панели слева выберите группу администрирования, содержащую устройство, к которому вы хотите получить доступ.
7. Установите флажок напротив устройства, к которому вы хотите получить доступ.
8. Нажмите на кнопку **Совместный доступ к рабочему столу Windows**.

   Открывается мастер Совместный доступ к рабочему столу Windows.
9. Нажмите на кнопку **Загрузить**, чтобы загрузить утилиту klsctunnel, и дождитесь завершения процесса загрузки.

   Если у вас уже есть утилита klsctunnel, пропустите этот шаг.
10. Нажмите на кнопку **Далее**.
11. Выберите сеанс на устройстве, к которому вы хотите подключиться, а затем нажмите на кнопку **Далее**.

12. 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.

13. 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.

14. Запустите утилиту klsctunnel.

    Откроется окно утилиты.

15. Вставьте скопированный текст в текстовое поле.

16. Если вы используете прокси-сервер, установите флажок **Использовать прокси-сервер**, а затем укажите параметры подключения к прокси-серверу.

17. 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**.

Выборки устройств

Выборки устройств – это инструмент для фильтрации устройств в соответствии с заданными условиями. Вы можете использовать выборки устройств, чтобы управлять несколькими устройствами: например, для просмотра отчетов только о выбранных устройствах или для перемещения всех этих устройств в другую группу администрирования.

Kaspersky Security Center предоставляет широкий диапазон *предопределенных выборок устройств* (например, **Устройства со статусом "Критический"**, **Защита выключена**, **Обнаружены активные угрозы**). Предопределенные выборки невозможно удалить. Вы можете также создавать и настраивать дополнительные *пользовательские выборки событий*.

В пользовательских выборках вы можете задать область поиска и выбрать все устройства, управляемые устройства или нераспределенные устройства. Параметры поиска задаются в условиях. В выборках устройств вы можете создать несколько условий с различными параметрами поиска. Например, вы можете создать два условия и задать различные IP-диапазоны в каждом из них. Если задано несколько условий, в выборку устройств попадут устройства, которые удовлетворяют любому из условий. Напротив, параметры поиска в одном условии накладываются друг на друга. Если в условии выборки заданы IP-диапазон и название установленного приложения, то в выборку устройств попадут только те устройства, на которых одновременно установлено указанное приложение и их IP-адреса входят в указанный диапазон.

Просмотр списка устройств из выборки устройств

Kaspersky Security Center позволяет просматривать список устройств из выборки устройств.

Чтобы просмотреть список устройств из выборки устройств:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Выборки устройств** или 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 **Активы (Устройства)** → **Выборки устройств**.

   Отобразится страница со списком выборок устройств.

2. Нажмите на кнопку **Добавить**.

   Откроется окно **Параметры выборки устройств**.

3. Введите имя новой выборки.

4. Укажите группу, содержащую устройства, которые будут включены в выборку устройств:

   - **Искать любые устройства** – поиск устройств, соответствующих критериям выборки, в группах **Управляемые устройства** или **Нераспределенные устройства**.
   - **Искать 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 **Активы (Устройства)** → **Выборки устройств**.

   Отобразится страница со списком выборок устройств.

2. Выберите соответствующую пользовательскую выборку устройств и нажмите на кнопку **Свойства**.

   Откроется окно **Параметры выборки устройств**.

3. На вкладке **Общие** перейдите по ссылке **Новое условие**.

4. Укажите условия, которые должны быть выполнены, чтобы устройство было включено в эту выборку.

5. Нажмите на кнопку **Сохранить**.

Параметры применены и сохранены.

Ниже описаны параметры условий отнесения устройств к выборке. Условия сочетаются по логическому "или": в выборку попадают устройства, удовлетворяющие хотя бы одному из представленных условий.

Общие

В разделе **Общие** можно изменить имя условия выборки и указать, необходимо ли инвертировать это условие:

Инвертировать условие выборки

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 **Контроллеры домена** можно настроить критерии включения устройств в выборку по членству в домене:

- **Устройство в подразделении домена**

  Если этот параметр включен, в выборку будут включаться устройства из подразделения домена, указанного в поле ввода.

  По умолчанию параметр выключен.

- **Это устройство является членом группы безопасности домена**

  Если этот параметр включен, в выборку будут включаться устройства из группы безопасности домена, указанной в поле ввода.

  По умолчанию параметр выключен.

В разделе **Сетевая активность** можно настроить критерии включения устройств в выборку на основании их сетевой активности:

- **Является точкой распространения**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Да**. В выборку будут включены устройства, являющиеся точками распространения.
  - **Нет**. Устройства, являющиеся точками распространения, не будут включены в выборку.
  - **Значение не выбрано**. Критерий не применяется.

- **Не разрывать соединение с Сервером администрирования**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Включен**. Выборка будет включать устройства, для которых установлен флажок **Не разрывать соединение с Сервером администрирования**.
  - **Выключен**. Выборка будет включать устройства, для которых снят флажок **Не разрывать соединение с Сервером администрирования**.
  - **Значение не выбрано**. Критерий не применяется.

- **Переключение профиля подключения**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Да**. В выборку будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
  - **Нет**. В выборку не будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
  - **Значение не выбрано**. Критерий не применяется.

- **Последнее подключение к Серверу администрирования**

  С помощью этого флажка можно задать критерий поиска устройств по времени последнего соединения с Сервером администрирования.

  Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее соединение установленного на клиентском устройстве Агента администрирования с Сервером администрирования. В выборку будут включены устройства, соответствующие установленному интервалу.

  Если флажок снят, то критерий не применяется.

  По умолчанию флажок снят.

- **Новые устройства, обнаруженные при опросе сети**

  Поиск новых устройств, обнаруженных при опросе сети за последние несколько дней.

  Если этот параметр включен, то в выборку попадают только новые устройства, найденные в процессе обнаружения устройств за количество дней, которое указано в поле **Период обнаружения (сут)**.

  Если этот параметр выключен, то в выборку попадают все устройства, найденные в процессе обнаружения устройств.

  По умолчанию параметр выключен.

- **Устройство в сети**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Да**. 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, Остановлен, Запускается, Приостановлен, Выполняется, Сбой*).

- **Статус защиты для серверов совместной работы**

  Поиск устройств по статусу защиты для серверов совместной работы (*Нет данных*, *Остановлен*, *Запускается, Приостановлен*, *Выполняется*, *Сбой*).

- **Статус антивирусной защиты почтовых серверов**

  Поиск устройств по статусу защиты почтовых серверов (*Нет данных, Остановлен, Запускается, Приостановлен, Выполняется, Сбой*).

- **Статус Endpoint Sensor**

  Поиск устройств по статусу компонента Endpoint Sensor (*Нет данных, Остановлен, Запускается, Приостановлен, Выполняется, Сбой*).

В разделе **Проблемы, связанные со статусом управляемых приложений** можно настроить критерии включения устройств в выборку в соответствии со списком возможных проблем, обнаруженных управляемым приложением. Если на устройстве существует хотя бы одна проблема, которую вы выбирали, устройство будет включено в выборку. Когда вы выбираете проблему, указанную для нескольких приложений, у вас есть возможность автоматически выбрать эту проблему во всех списках.

Вы можете установить флажки для описаний статусов от управляемого приложения, при получении которых устройства будут включаться в выборку. Когда вы выбираете статус, указанный для нескольких приложений, у вас есть возможность автоматически выбирать этот статус во всех списках.

Сведения о системе

В разделе **Операционная система** можно настроить критерии включения устройств в выборку на основании установленной на них операционной системы.

- **Тип платформы**

  Если флажок установлен, в списке можно выбрать операционные системы. Устройства, на которых установлены указанные операционные системы, включаются в результаты поиска.

- **Версия пакета обновления операционной системы**

  В поле можно указать версию пакета установленной операционной системы (в формате *X.Y*), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

- **Архитектура операционной системы**

  В раскрывающемся списке можно выбрать архитектуру операционной системы, по наличию которой к устройству применяется правило перемещения (**Нет данных**, **x86**, **AMD64** или **IA64**). По умолчанию в списке не выбран ни один вариант, архитектура операционной системы не задана.

- **Номер сборки операционной системы**

  > Этот параметр применим только для операционных систем Windows.

  Номер сборки операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить поиск всех номеров сборки, кроме указанного.

- **Номер выпуска операционной системы**

  > Этот параметр применим только для операционных систем Windows.

Идентификатор выпуска операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний идентификатор выпуска. Вы также можете настроить поиск всех номеров идентификаторов выпуска, кроме указанного.

В разделе **Виртуальные машины** можно настроить критерии включения устройств в выборку в зависимости от того, являются эти устройства виртуальными машинами или частью Virtual Desktop Infrastructure:

- **Является виртуальной машиной**

  В раскрывающемся списке можно выбрать следующие элементы:

  - **Не определено**.
  - **Нет**. Искомые устройства не должны являться виртуальными машинами.
  - **Да**. Искомые устройства должны являться виртуальными машинами.

- **Тип виртуальной машины**

  В раскрывающемся списке можно выбрать производителя виртуальной машины.

  Этот список доступен, если в раскрывающемся списке **Является виртуальной машиной** выбрано значение **Да** или **Неважно**.

- **Часть Virtual Desktop Infrastructure**

  В раскрывающемся списке можно выбрать следующие элементы:

  - **Не определено**.
  - **Нет**. Искомые устройства не должны являться частью Virtual Desktop Infrastructure.
  - **Да**. Искомые устройства должны являться частью Virtual Desktop Infrastructure (VDI).

В разделе **Реестр оборудования** можно настроить критерии включения устройств в выборку по установленному на них оборудованию:

Убедитесь, что утилита lshw установлена на устройствах Linux, с которых вы хотите получить информацию об оборудовании. Сведения об оборудовании, полученные с виртуальных машин, могут быть неполными в зависимости от используемого гипервизора

- **Устройство**

  В раскрывающемся списке можно выбрать тип оборудования. Все устройства с таким оборудованием включены в результат поиска.

  В поле поддерживается полнотекстовый поиск.

- **Поставщик**

  В раскрывающемся списке можно выбрать имя производителя оборудования. Все устройства с таким оборудованием включены в результат поиска.

  В поле поддерживается полнотекстовый поиск.

- **Имя устройства**

  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:

  - **Да**. Приложение включает в выборку устройства, которые находятся под управлением Kaspersky Security Center.
  - **Нет**. Приложение включает в выборку устройства, которые не находятся под управлением Kaspersky Security Center.
  - **Значение не выбрано**. Критерий не применяется.

- **Приложение безопасности установлено**

  В раскрывающемся списке можно включить в состав выборки устройства, на которых установлено приложение безопасности:

  - **Да**. Приложение включает в выборку устройства, на которых установлено приложение безопасности.
  - **Нет**. Приложение включает в выборку устройства, на которых не установлено приложение безопасности.
  - **Значение не выбрано**. Критерий не применяется.

В разделе **Антивирусная защита** можно настроить критерии включения устройств в выборку по состоянию защиты:

- **Дата выпуска баз**

  Если этот параметр выбран, поиск клиентских устройств выполняется по дате выпуска антивирусных баз. В полях ввода можно задать временной интервал, на основании которого будет выполняться поиск.

  По умолчанию параметр выключен.

- **Количество записей в базах**

  Если этот параметр включен, поиск клиентских устройств выполняется по количеству записей в базе. В полях ввода можно задать нижнее и верхнее значения количества записей антивирусной базы.

  По умолчанию параметр выключен.

- **Последняя проверка**

  Если этот параметр включен, поиск клиентских устройств выполняется по времени последнего поиска вредоносного ПО. В полях ввода можно указать интервал, в течение которого поиск вредоносного ПО выполнялся в последний раз.

  По умолчанию параметр выключен.

- **Обнаружены угрозы**

  Если этот параметр включен, поиск клиентских устройств выполняется по количеству найденных вирусов. В полях ввода можно задать нижнее и верхнее значения количества найденных вирусов.

  По умолчанию параметр выключен.

В подразделе **Шифрование** можно настроить критерии включения устройств в выборку на основе выбранного алгоритма шифрования:

Алгоритм шифрования

Стандарт симметричного алгоритма блочного шифрования Advanced Encryption Standard (AES). В раскрывающемся списке вы можете выбрать размер ключа шифрования (56 Бит, 128 Бит, 192 Бит или 256 Бит).

Доступные значения: *AES56*, *AES128*, *AES192*, и *AES256*.

Подраздел **Компоненты приложения** содержит список компонентов тех приложений, которые имеют соответствующие плагины управления, установленные в Kaspersky Security Center Web Console.

В разделе **Компоненты приложения** вы можете задать критерий для включения устройств в выборку в соответствии с номерами версий компонентов, относящихся к выбранному приложению:

- **Статус**

  Поиск устройств в соответствии со статусом компонента, отправленным управляемым приложением на Сервер администрирования. Вы можете выбрать один из следующих статусов: *Нет данных от устройства*, *Остановлен*, *Приостановлено*, *Запускается*, *Выполняется*, *Сбой*, *Не установлен*, *Не поддерживается лицензией*. Если выбранный компонент приложения, установленный на управляемом устройстве, имеет указанный статус, устройство входит в выборку устройств.

  Статусы, отправленные приложениями:

  - *Остановлено* – компонент отключен и в данный момент не работает.
  - *Приостановлено* – компонент приостановлен, например, после того, как пользователь приостановил защиту в управляемом приложении.
  - *Запускается* – компонент в настоящее время находится в процессе инициализации.
  - *Выполняется* – компонент включен и работает правильно.
  - *Сбой* – во время выполнения операции компонента произошла ошибка.
  - *Не установлено* – пользователь не выбрал компонент для установки во время выборочной установки приложения.
  - *Не поддерживается лицензией* – лицензия не распространяется на выбранный компонент.

  В отличие от других статусов, статус *Нет данных от устройства* не отправляется управляемым приложением. Этот параметр показывает, что приложения не имеют информации о выбранном статусе компонента. Например, это может произойти, если выбранный компонент не принадлежит ни одному из приложений, установленных на устройстве, или устройство выключено.

- **Версия**

  Поиск устройств в соответствии с номером версии компонента, который вы выбрали в списке. Вы можете ввести номер версии, например, `3.4.1.0`, а затем указать, должен ли выбранный компонент иметь равную, более раннюю или более позднюю версию. Также вы можете настроить поиск по всем версиям компонента, кроме указанной.

Теги

В разделе **Теги** можно настроить критерии включения устройств в выборку по ключевым словам (тегам), которые были добавлены ранее в описания управляемых устройств:

Применить, если есть хотя бы один из выбранных тегов

Если этот параметр включен, в результатах поиска отобразятся устройства, в описании которых есть хотя бы один из выбранных тегов.

Если этот параметр выключен, в результатах поиска отобразятся только устройства, в описаниях которых есть все выбранные теги.

По умолчанию параметр выключен.

Чтобы добавить теги к критерию, нажмите на кнопку **Добавить** и выберите теги, нажав на поле ввода **Тег**. Укажите, следует ли включать или исключать устройства с выбранными тегами в выборку устройств.

- **Все устройства, имеющие этот тег**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых есть выбранный тег. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

  По умолчанию выбран этот вариант.

- **Все устройства, не имеющие этого тега**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых нет выбранного тега. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

Пользователи

В разделе **Пользователи** можно настроить критерии включения устройств в выборку по учетным записям пользователей, выполнявших вход в операционную систему.

- **Последний пользователь, выполнивший вход в систему**

  Если этот параметр включен, вы можете выбрать учетную запись пользователя, для которой настроили критерий. В результаты поиска включаются устройства, на которых последний вход в систему выполнялся выбранным пользователем.

- **Пользователь, уже выполнявший вход в систему**

  Если этот параметр включен, при нажатии на кнопку **Обзор** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых указанный пользователь когда-либо выполнял вход в систему.

Экспорт списка устройств из выборки устройств

Kaspersky Security Center позволяет сохранять информацию об этих устройствах из выборки устройств и экспортировать ее в файл CSV или TXT.

Чтобы экспортировать список устройств из выборки устройств:

1. Откройте таблицу с устройствами из выборки устройств.
2. Используйте один из следующих способов для выбора устройств, которые вы хотите экспортировать:
   - Чтобы выбрать определенные устройства, установите флажки рядом с ними.
   - Чтобы выбрать все устройства на текущей странице таблицы, установите флажок в заголовке таблицы устройств, а затем установите флажок **Выбрать все на текущей странице**.
   - Чтобы выбрать все устройства из таблицы, установите флажок в заголовке таблицы устройств, а затем выберите **Выбрать все**.
3. Нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**. Вся информация о выбранных устройствах, включенных в таблицу, будет экспортирована.

Обратите внимание, если вы отфильтровали таблицу устройств, будут экспортированы только отфильтрованные данные отображаемых столбцов.

Удаление устройств из групп администрирования в выборке

При работе с выборкой устройств вы можете удалять устройства из групп администрирования прямо в выборке, не переходя к работе с группами администрирования, из которых требуется удалить устройства.

Чтобы удалить устройства из групп администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Выборки устройств** или **Обнаружение устройств и развертывание** → **Выборки устройств**.
2. В списке выборок нажмите на имя выборки устройств.

   На странице отображается таблица с информацией об устройствах, включенных в выборку устройств.
3. Выберите устройства, которые вы хотите удалить и нажмите на кнопку **Удалить**.

   В результате выбранные устройства будут удалены из групп администрирования, в которые они входили.

Теги устройств

Kaspersky Security Center позволяет назначать *теги* устройствам. Тег представляет собой идентификатор устройства, который можно использовать для группировки, описания, поиска устройств. Назначенные устройствам теги можно использовать при создании выборок устройств, при поиске устройств и при распределении устройств по группам администрирования.

Теги могут назначаться устройствам вручную или автоматически. Если вы хотите отметить отдельное устройство, вы можете назначить тег вручную. Автоматическое назначение тегов выполняется Kaspersky Security Center одним из следующих способов:

- В соответствии с указанными правилами назначения тегов.
- В соответствии с указанным приложением.

Не рекомендуется использовать разные способы назначения тегов для назначения одного и того же тега. Например, если тег назначается правилом, не рекомендуется назначать этот тег устройствам вручную.

Если теги назначаются правилами, устройствам назначаются теги автоматически при соблюдении указанных правил. Каждому тегу соответствует отдельное правило. Правила могут применяться к сетевым свойствам устройства, операционной системе, установленным на устройстве приложениям и другим свойствам устройства. Например, если используется гибридная инфраструктура, состоящая из физических устройств, инстансов Amazon EC2 и виртуальных машин Microsoft Azure, можно настроить правило, в соответствии с которым всем виртуальным машинам Microsoft Azure будет назначен тег `[Azure]`. Затем можно использовать этот тег при создании выборки устройств, чтобы отобрать все виртуальные машины Microsoft Azure 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 **Активы (Устройства)** → **Теги** → **Теги устройств**.
2. Нажмите на кнопку **Добавить**.

   Отобразится окно создания тега.
3. В поле **Тег** введите название тега.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Новый созданный тег появляется в списке тегов устройства.

Изменение тегов устройств

Чтобы переименовать тег устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Теги** → **Теги устройств**.
2. Выделите тег, который требуется переименовать.

   Откроется окно свойств тега.
3. В поле **Тег** измените название тега.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Обновленный тег появится в списке тегов устройства.

Удаление тегов устройств

Чтобы удалить тег устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Теги** → **Теги устройств**.
2. В списке выберите теги устройства, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить**.
4. В 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 **Активы (Устройства)** → **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 **Управляемые устройства** главного меню с устройствами, отфильтрованными по тегу, для которого вы нажали ссылку **Просмотреть устройства**.
3. Если вы хотите вернуться к списку тегов устройства, нажмите на кнопку **Назад** в браузере.

После просмотра устройств, которым назначен тег, вы можете создать и назначить новый тег или назначить существующий тег другим устройствам. В этом случае вам придется удалить фильтр по тегу, выбрать устройства и назначить тег.

Просмотр тегов, назначенных устройству

Чтобы просмотреть теги, назначенные устройству:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. Выберите устройство, теги которого требуется просмотреть.
3. В открывшемся окне свойств устройства выберите вкладку **Теги**.

   Отобразится список тегов, назначенных выбранному устройству. В столбце **Назначенный тег** вы можете просмотреть, как был назначен тег.

В панели инструментов можно выполнить следующие действия:

- Назначить устройству другой тег.
- Удалить уже назначенный тег.
- Просмотреть все теги устройств, которые существуют на Сервере администрирования.

> Вы не можете просматривать назначенные теги локально на устройстве.

Назначение тегов устройству вручную

Чтобы вручную назначить тег устройству:

1. Просмотрите теги, уже назначенные устройству, которому вы ходите назначить тег.
2. Нажмите на кнопку **Добавить**.

3. В открывшемся окне выполните одно из следующих действий:

   - Чтобы создать и назначить новый тег, выберите пункт **Создать тег** и укажите тег.
   - Чтобы выбрать существующий тег, выберите пункт **Назначить существующий тег** и в раскрывающемся списке выберите нужный тег.

4. Нажмите на кнопку **OK**, чтобы применить изменения.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Выбранный тег будет назначен устройству.

Удаление назначенного тега с устройства

Чтобы снять назначенный тег с устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.

2. Выберите устройство, теги которого требуется просмотреть.

3. В открывшемся окне свойств устройства выберите вкладку **Теги**.

4. Установите флажок напротив тега, который требуется снять.

5. В верхней части списка нажмите на кнопку **Отменить назначение тега?**.

6. В появившемся окне нажмите на кнопку **Да**.

Тег будет снят с устройства.

Снятый с устройства тег не удаляется. При необходимости его можно удалить вручную.

Вы не можете вручную удалить теги, назначенные устройству приложениями или Агентом администрирования. Для того чтобы управлять этими тегами, используйте утилиту klscflag.

Просмотр правил автоматического назначения тегов устройствам

Чтобы просмотреть правила автоматического назначения тегов устройствам,

Выполните одно из следующих действий:

- В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Теги** → **Правила автоматического назначения тегов**.
- В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Теги** → **Теги устройств**, а затем перейдите по ссылке **Настроить правила автоматического назначения тегов**.
- Перейдите к просмотру тегов, назначенных устройству, 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, настроена сортировка с учетом регистра, учитывайте регистр при указании DNS-имени устройства. Иначе правила автоматического назначения тегов не будет работать.

   - **Приложения** – наличие на устройстве Агента администрирования, тип, версия и архитектура операционной системы.

   - **Виртуальные машины** – принадлежность устройства к определенному типу виртуальных машин.

- **Контроллеры домена** – 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 теги вашему устройству с помощью утилиты klscflag:

1. Запустите командную строку Windows с правами администратора, а затем измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в папке установки Агента администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\NetworkAgent.

2. Введите одну из следующих команд:

   - Чтобы назначить набор тегов:

     ```
     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:

     ```
     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:

     ```
     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:

```
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.

Политики и профили политик

В Kaspersky Security Center Web Console можно создавать политики для приложений "Лаборатории Касперского". В этом разделе описаны политики и профили политик, а также приведены инструкции по их созданию и изменению.

О политиках и профилях политик

Политика – это набор параметров приложения "Лаборатории Касперского", которые применяются к группе администрирования и ее подгруппе. Вы можете установить несколько приложений "Лаборатории Касперского" на устройства группы администрирования. Kaspersky Security Center предоставляет по одной политике для каждого приложения "Лаборатории Касперского" в группе администрирования. Политика имеет один из следующих статусов (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.

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:

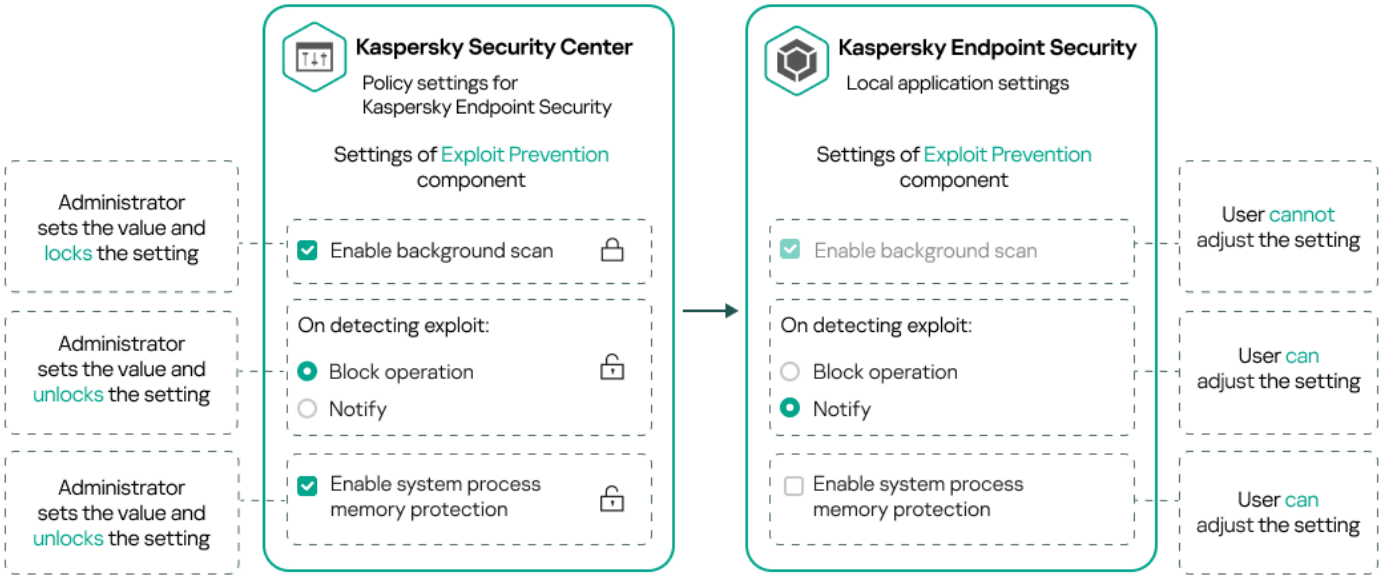
- Блокировка параметров для политики подгруппы администрирования.
- Блокировка параметров приложения "Лаборатории Касперского" на управляемом устройстве.

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

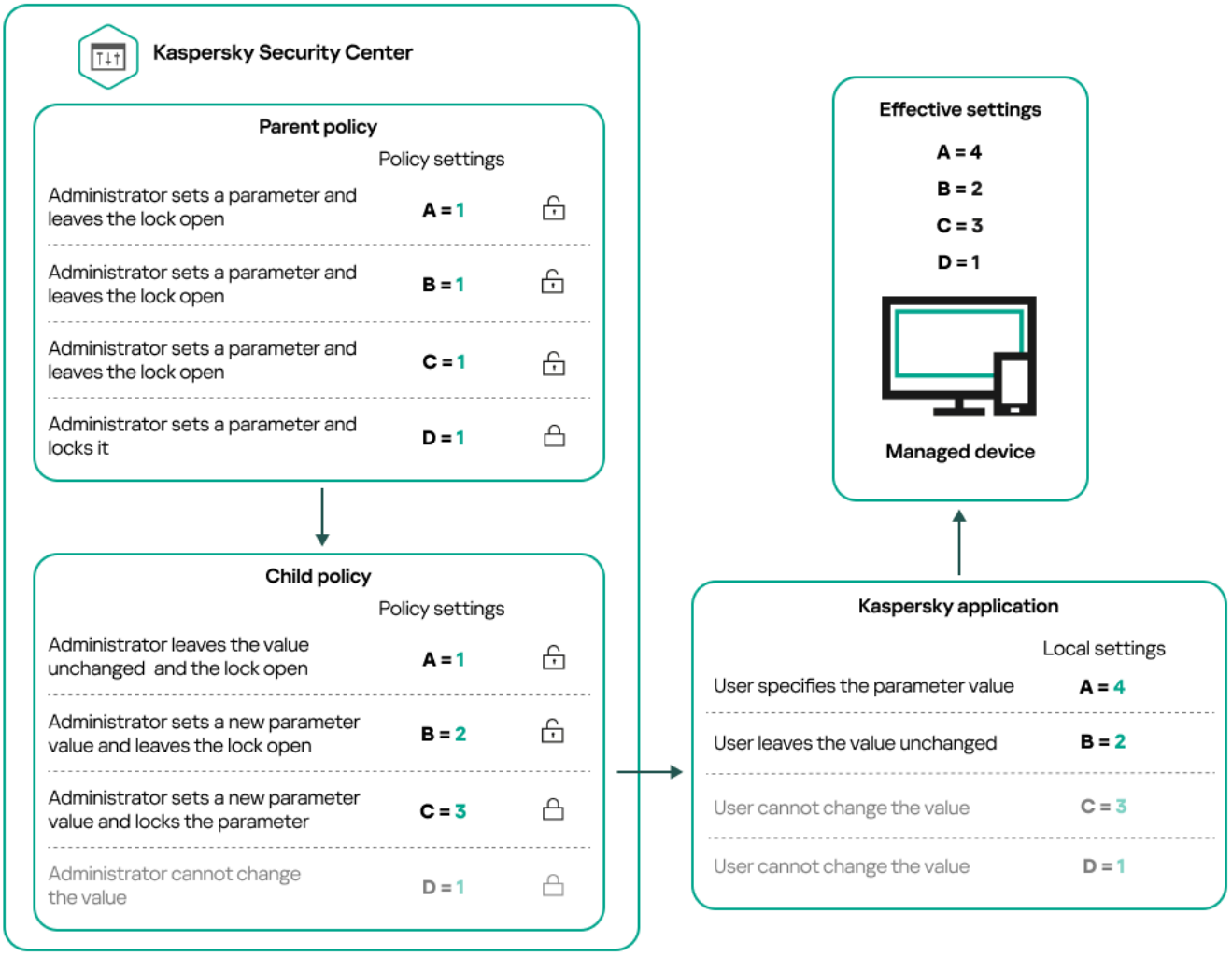
Если для разных устройств требуются разные параметры, вы можете объединить устройства в группы администрирования.

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).

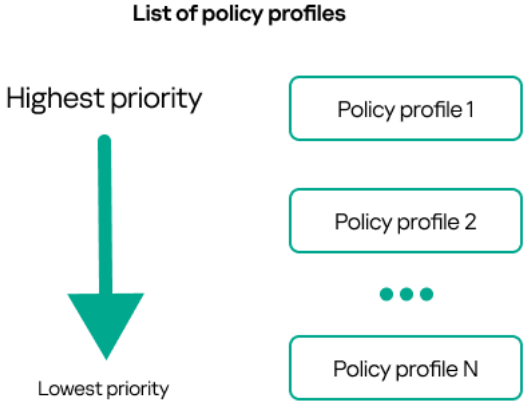


Иерархия политик

Профили политик в иерархии политик

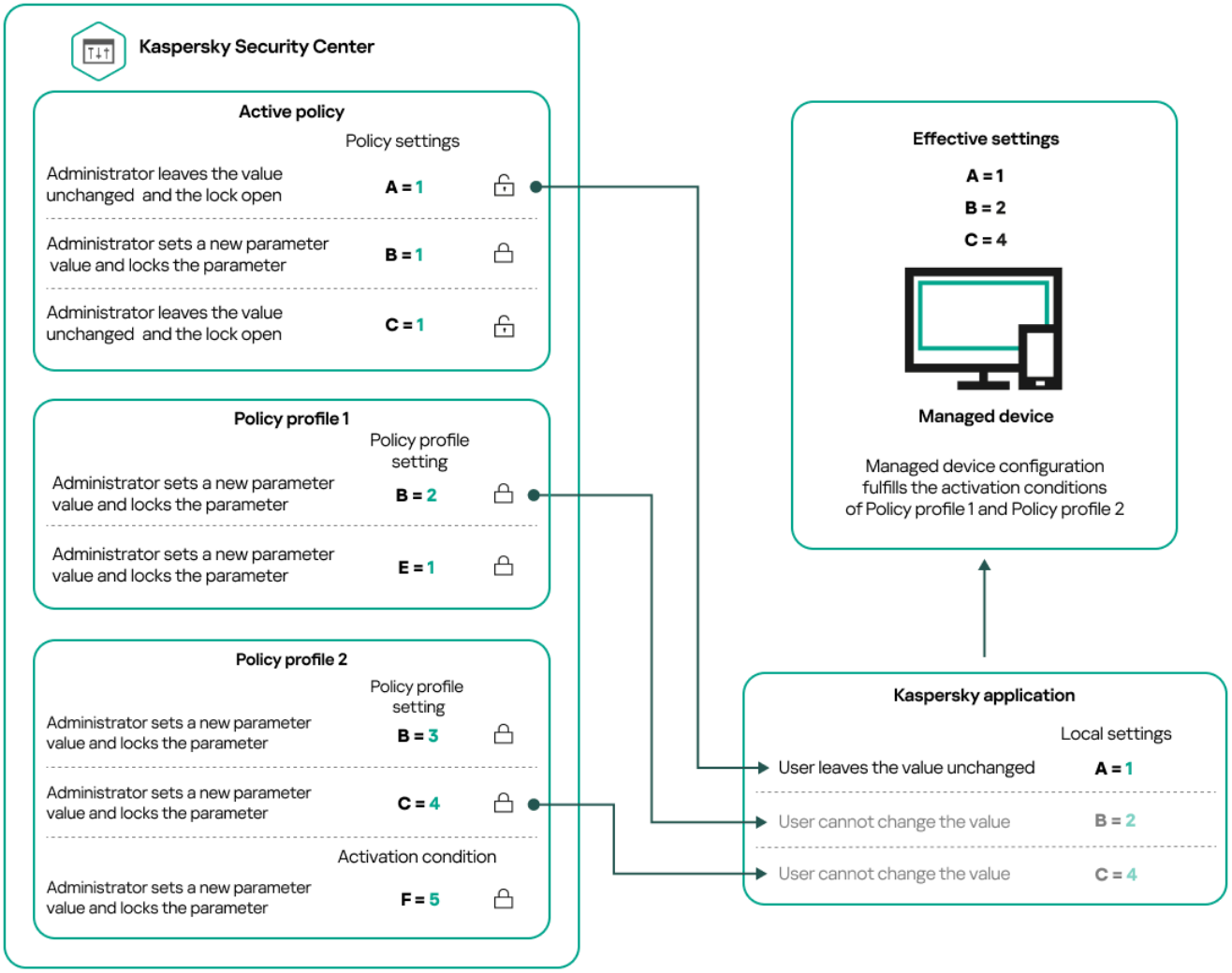
Профили политики имеют следующие условия назначения приоритета:

- 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).



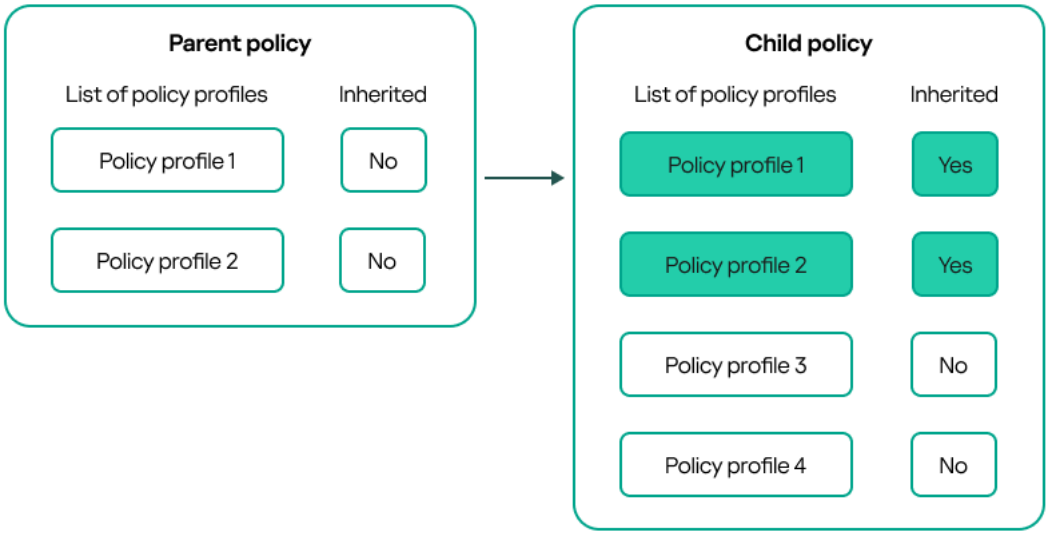
Конфигурация управляемого устройства соответствует условиям активации нескольких профилей политик

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).

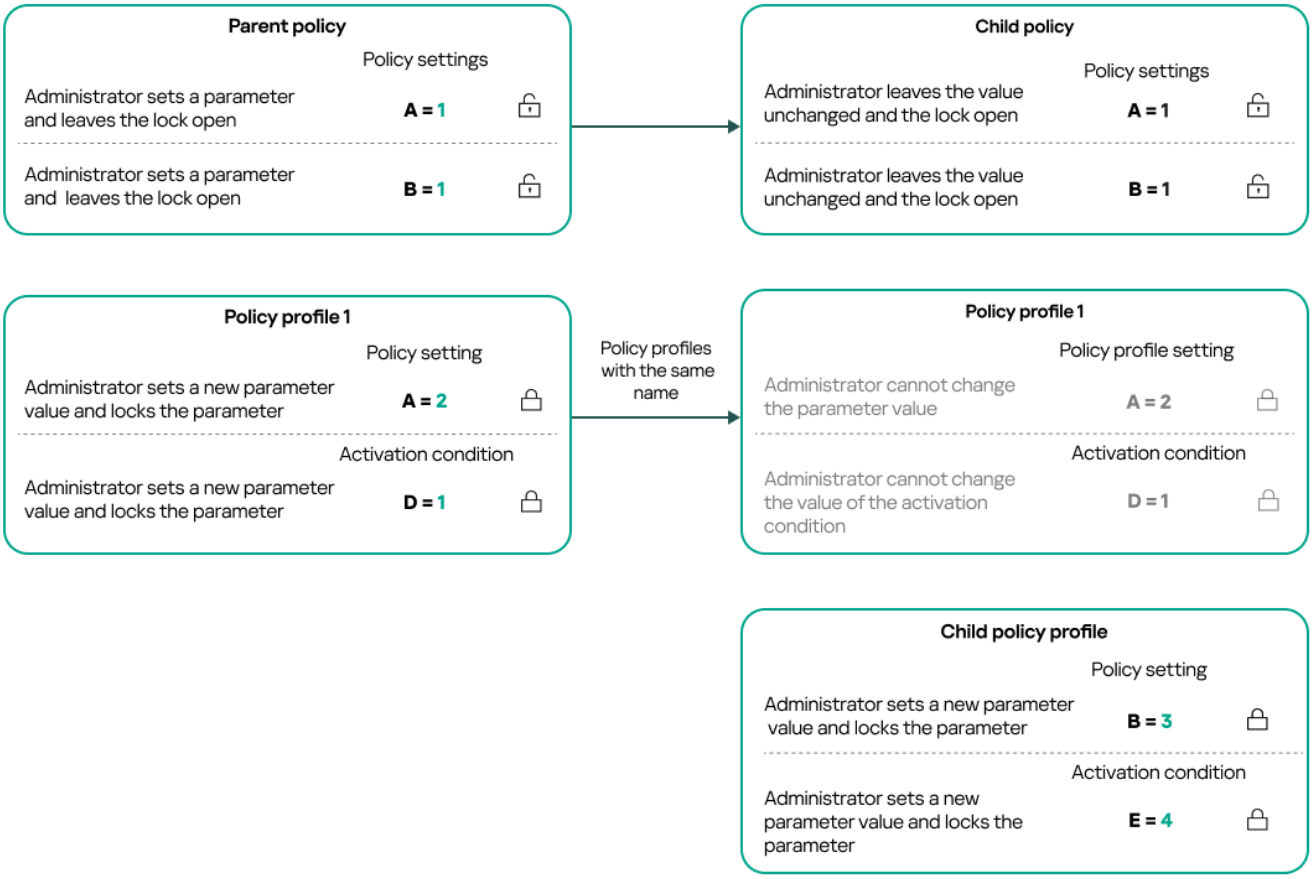


Наследование параметров профилей политики

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 **Активы (Устройства)** → **Иерархия групп**.
2. В списке групп администрирования выберите группу администрирования, для которой вы хотите просмотреть список политик.

Политики отобразятся в виде таблицы. Если политик нет, отобразится пустая таблица. Вы можете отображать или скрывать столбцы таблицы, изменять их порядок, просматривать только строки, которые содержат указанное вами значение, или использовать поиск.

Создание политики

Вы можете создавать политики; вы можете также изменять или удалять существующие политики.

Чтобы создать политику:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Выберите группу администрирования, для которой нужно создать политику:
   - Для корневой группы.

     В этом случае вы можете перейти к следующему шагу.
   - Для подгруппы:

     a. Нажмите на ссылку текущего пути в верхней части окна.

     b. В открывшейся панели нажмите на ссылку с названием нужной подгруппы.

     Текущий путь изменится в соответствии с выбранной подгруппой.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Выберите 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.

   Набор параметров зависит 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 **Активы (Устройства)** → **Политики и профили политик**.
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**.

Изменения политики будут сохранены в свойствах политики и будут отображаться в разделе **История ревизий**.

Общие параметры политик

Общие

На вкладке **Общие** можно изменить состояние политики и настроить наследование параметров политики:

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:
  - **Активна**

    Если выбран этот вариант, политика становится активной.

    По умолчанию выбран этот вариант.
  - **Для автономных пользователей**

    Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.
  - **Неактивна**

    Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.
- В блоке **Наследование параметров** можно настроить параметры наследования политики:
  - **Наследовать параметры родительской политики**

    Если параметр включен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

    По умолчанию параметр включен.
  - **Обеспечить принудительное наследование параметров для дочерних политик**

    Если параметр включен, после применения изменений в политике будут выполнены следующие действия:
    - значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
    - в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически включен параметр **Наследовать параметры родительской политики**.

    Когда параметр включен, значения параметров дочерних политик недоступны для изменения.

    По умолчанию параметр выключен.

Настройка событий

На вкладке **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на вкладках:

- **Критическое**

  Раздел **Критическое** не отображается в свойствах политики Агента администрирования.
- **Отказ функционирования**
- **Предупреждение**
- **Информационное сообщение**

В каждом разделе в списке событий отображаются названия событий и время хранения событий на Сервере администрирования по умолчанию (в днях). Нажав на тип события, вы можете указать следующие параметры:

- **Регистрация событий**

  Вы можете указать количество дней хранения событий и выбрать, где хранить события:

  - **Экспортировать в SIEM-систему по протоколу Syslog**
  - **Хранить в журнале событий ОС на устройстве**
  - **Хранить в журнале событий ОС на Сервере администрирования**

- **Уведомления о событиях**

  Вы можете выбрать способ уведомления о событии:

  - **Уведомлять по электронной почте**
  - **Уведомлять по SMS**
  - **Уведомлять запуском исполняемого файла или скрипта**
  - **Уведомлять по SNMP**

  По умолчанию используются параметры уведомлений, указанные на вкладке свойств Сервера администрирования (например, адрес получателя). Если вы хотите, измените эти параметры на вкладках **Электронная почта**, **SMS** и **Исполняемый файл для запуска**.

История ревизий

На вкладке **История ревизий** вы можете просмотреть список ревизий политики и изменения, для которых был выполнен откат.

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 **Активы (Устройства)** → **Политики и профили политик**.

2. Установите флажок напротив политики (или политик), которую требуется скопировать.

3. Нажмите на кнопку **Копировать**.

   В правой части экрана отображается дерево групп администрирования.

4. В дереве выберите целевую группу, то есть группу, в которую вы хотите скопировать политику (или политики).

5. Нажмите на кнопку **Копировать** внизу экрана.

6. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.

Политика (политики) и все ее профили скопированы в целевую группу администрирования. Каждая скопированная политика в целевой группе принимает статус **Неактивна**. Вы можете изменить статус политики на **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 **Активы (Устройства)** → **Политики и профили политик**.
2. Установите флажок напротив политики (или политик), которую требуется переместить.
3. Нажмите на кнопку **Переместить**.

   В правой части экрана отображается дерево групп администрирования.
4. В дереве выберите целевую группу администрирования, то есть группу, в которую вы хотите переместить политику (или политики).
5. Нажмите на кнопку **Переместить** внизу экрана.
6. Нажмите на кнопку **OK**, чтобы подтвердить операцию.

Если политика не унаследована из группы источника, она будет перемещена в целевую группу со всем профилями политики. Статус политики в целевой группе администрирования будет **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

Если политика унаследована из группы источника, она останется в группе источника. Политика скопирована в целевую группу со всеми ее профилями. Статус политики в целевой группе администрирования будет **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

Если в целевой группе политик уже существует политика с именем, совпадающим с именем копируемой политики, к имени копируемой политики будет добавлено окончание вида (<следующий порядковый номер>), например: (1).

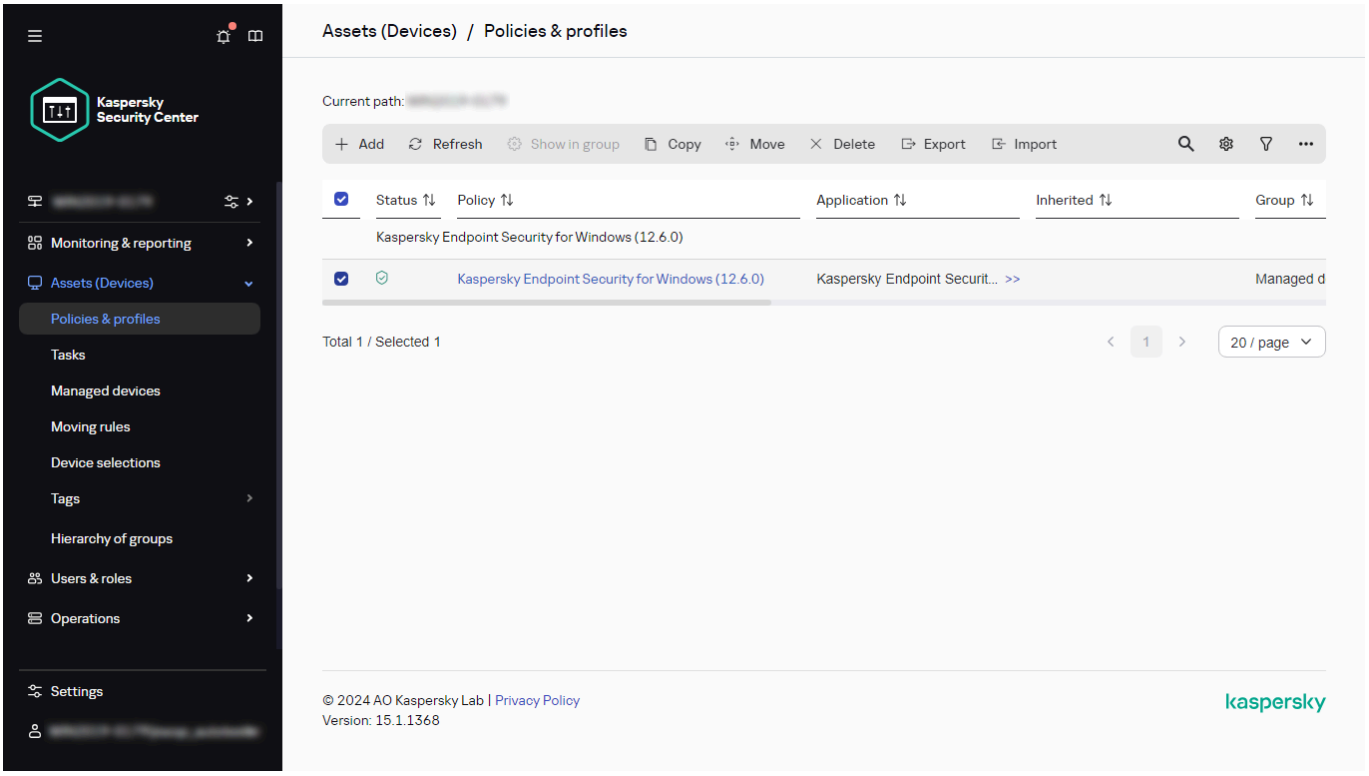
Экспорт политики

Kaspersky Security Center 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 **Активы (Устройства)** → **Политики и профили политик**.
2. Установите флажок рядом с политикой, которую вы хотите экспортировать.

Невозможно экспортировать несколько политик одновременно. Если вы выберете более одной политики, кнопка **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 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 **Активы (Устройства)** → **Политики и профили политик**.

2. Нажмите на кнопку **Импортировать**.

3. Нажмите на кнопку **Обзор**, чтобы выбрать файл политики, который вы хотите импортировать.

4. В открывшемся окне укажите путь к файлу политики KLP и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл политики.

   Начнется обработка политики.

5. После успешной обработки политики выберите группу администрирования, к которой вы хотите применить политику.

6. Нажмите на кнопку **Завершить**, чтобы завершить импорт политики.

Появится уведомление с результатами импорта. Если политика успешно импортирована, вы можете перейти по ссылке **Подробнее** для просмотра свойств политики.

После успешного импорта политика отображается в списке политик. Также импортируются параметры и профили политики. Независимо от статуса политики, выбранной при экспорте, импортируемая политика неактивна. Вы можете изменить статус политики в свойствах политики.

Если параметры политики приложения содержат пароли, такую политику невозможно применить после импорта на другой Сервер Администрирования. В этом случае измените пароли в импортированной политике для ее применения.

Если имя новой импортированной политики идентично имени существующей политики, имя импортированной политики расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Просмотр диаграммы состояния применения политики

В Kaspersky Security Center вы можете просматривать состояние применения политики на каждом устройстве на диаграмме.

Чтобы просмотреть статус применения политики на каждом устройстве:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Установите флажок рядом с именем политики, для которой вы хотите просмотреть состояние применения на устройстве.
3. В появившемся меню выберите ссылку **Результаты применения**.

   Откроется окно **Результат распространения <название политики>**.
4. В открывшемся окне **Результат распространения <название политики>** отображается **Описание статуса**.

Вы можете изменить количество результатов, отображаемых в списке результатов применения политики. Максимальное количество устройств равно 100 000.

Чтобы изменить количество устройств, отображаемых в списке с результатами применения политики:

1. В главном меню перейдите в параметры своей учетной записи и выберите **Параметры интерфейса.**
2. В поле **Максимальное количество устройств, отображаемых в результатах распространения политики** введите количество устройств (до 100 000).

   По умолчанию количество устройств равно 5000.
3. Нажмите на кнопку **Сохранить**.

   Параметры сохранены и применены.

Удаление политики

Вы можете удалить политику, если она больше не нужна. Вы можете удалить только неунаследованную политику в выбранной группе администрирования. Если политика унаследована, вы можете удалить ее только в группе администрирования, в которой она была создана.

Чтобы удалить политику:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Установите флажок рядом с именем политики, которую вы хотите удалить, и нажмите на кнопку **Удалить**.

   Кнопка **Удалить** становится неактивной (серой), если вы выбрали унаследованную политику.
3. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.

Политика и все ее профили политики удалены.

Управление профилями политик

В этом разделе описывается управление профилями политики и предоставляется информация о просмотре профилей политики, изменении приоритета профиля политики, создании профиля политики, изменении профиля политики, копировании профиля политики, создании правила активации профиля политики и удалении профиля политики.

Просмотр профилей политики

Чтобы просмотреть профили политики:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Выберите политику, профили которой требуется просмотреть.

   Откроется окно свойств политики на вкладке **Общие**.
3. Откройте вкладку **Профили политики**.

Профили политики отобразятся в виде таблицы. Если у политики нет профилей политики, отобразится пустая таблица.

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.

     - **Правило подключения к Серверу администрирования активно на этом устройстве**

       Выберите условие для активации профиля политики (независимо от того, выполняется ли это правило или нет) и выберите имя правила.

       Правило определяется сетевым местоположением устройства для подключения к Серверу администрирования, при выполнении или невыполнении условий которого профиль политики будет активирован.

       Описание сетевого местоположения устройств для подключения к Серверу администрирования можно создать или настроить в правиле переключения Агента администрирования.

   - **Правила для выбранного владельца устройства**

Для этого параметра на следующем шаге укажите:

- **Владелец устройства**

  Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по владельцу устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

  - устройство принадлежит указанному владельцу (знак "=");
  - устройство не принадлежит указанному владельцу (знак "#").

    Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать владельца устройства, когда параметр включен. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- **Владелец устройства включен во внутреннюю группу безопасности**

  Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по членству владельца устройства во внутренней группе безопасности Kaspersky Security Center. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

  - владелец устройства является членом указанной группы безопасности (знак "=");
  - владелец устройства не является членом указанной группы безопасности (знак "#").

    Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать группу безопасности Kaspersky Security Center. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- **Правила для характеристик оборудования**

  Установите флажок, чтобы настроить условие активации профиля политики на устройстве в зависимости от объема памяти и количества логических процессоров устройства.

  Для этого параметра на следующем шаге укажите:

  - **Объем оперативной памяти (МБ)**

    Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по объему оперативной памяти устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

    - объем оперативной памяти устройства меньше указанного значения (знак "<");
    - объем оперативной памяти устройства больше указанного значения (знак ">").

    Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать объем оперативной памяти устройства. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- **Количество логических процессоров**

  Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по количеству логических процессоров устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

  - количество логических процессоров устройства меньше или равно указанному значению (знак "<");
  - количество логических процессоров устройства больше или равно указанному значению (знак ">").

  Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать количество логических процессоров устройства. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- **Правила для назначения роли**

  Для этого параметра на следующем шаге укажите:

  Активировать профиль политики по наличию роли у владельца устройства

  Включите этот параметр, чтобы настроить и включить правило активации профиля политики на устройстве в зависимости от наличия определенной роли у его владельца. Добавить роль вручную из списка существующих ролей.

  Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием.

- **Правила для использования тега**

  Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от тегов, назначенных устройству. Вы можете активировать профиль политики либо на устройствах, которые имеют выбранные теги, либо не имеют их.

  Для этого параметра на следующем шаге укажите:

  - **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.

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

Можно управлять следующими типами шифрования:

- шифрование диска BitLocker на устройствах под управлением операционной системы Windows для серверов;
- шифрование диска Kaspersky на устройствах под управлением операционной системы Windows для рабочих станций.

С помощью этих компонентов Kaspersky Endpoint Security для Windows вы можете, например, включать или выключать шифрование, 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. 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. 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 вы можете просмотреть информацию о зашифрованных жестких дисках и об устройствах, зашифрованных на уровне дисков. После того, как информация на диске будет расшифрована, диск будет автоматически удален из списка.

Чтобы просмотреть список зашифрованных жестких дисков,

В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных** → **Зашифрованные жесткие диски**.

Если раздела нет в меню, значит, он скрыт. В настройках пользовательского интерфейса включите параметр **Показать раздел "Шифрование и защита данных"** для отображения раздела.

Вы можете экспортировать список зашифрованных жестких дисков в файлы форматов CSV или TXT. Для этого нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**.

Просмотр списка событий шифрования

В процессе выполнения задач шифрования или расшифровки данных на устройствах Kaspersky Endpoint Security для Windows отправляет в Kaspersky Security Center информацию о возникающих событиях следующих типов:

- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за нехватки места на диске;
- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за проблем с лицензией;
- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за отсутствия прав доступа;
- приложению запрещен доступ к зашифрованному файлу;
- неизвестные ошибки.

Чтобы просмотреть список событий, возникших при шифровании данных на устройствах:

В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных** → **События шифрования**.

Если раздела нет в меню, значит, он скрыт. В настройках пользовательского интерфейса включите параметр **Показать раздел "Шифрование и защита данных"** для отображения раздела.

Вы можете экспортировать список зашифрованных жестких дисков в файлы форматов CSV или TXT. Для этого нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**.

Также можно просмотреть список событий шифрования для каждого управляемого устройства.

Чтобы просмотреть события шифрования управляемого устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. Нажмите на имя управляемого устройства.
3. На вкладке **Общие** перейдите в раздел **Защита**.
4. Перейдите по ссылке **Просмотреть ошибки шифрования данных**.

Формирование и просмотр отчетов о шифровании

Вы можете формировать следующие отчеты:

- Отчет о статусе шифрования управляемых устройств. В этом отчете представлены сведения о шифровании данных различных управляемых устройств. Например, в отчете показано количество устройств, к которым применяется политика с настроенными правилами шифрования. Также можно узнать, например, сколько устройств нужно перезагрузить. Отчет также содержит информацию о технологии и алгоритме шифрования для каждого устройства.
- Отчет о статусе шифрования запоминающих устройств. Этот отчет содержит похожую информацию, что и отчет о состоянии шифрования управляемых устройств, но предоставляет данные только для запоминающих устройств и съемных дисков.
- Отчет о правах доступа к зашифрованным дискам. Этот отчет показывает, какие учетные записи пользователей имеют доступ к зашифрованным жестким дискам.
- Отчет об ошибках шифрования файлов. Отчет содержит информацию об ошибках, которые возникли при выполнении задач шифрования или расшифровки данных на устройствах.
- Отчет о блокировании доступа к зашифрованным файлам. Отчет содержит информацию о блокировке доступа приложений к зашифрованным файлам. Этот отчет полезен, если неавторизованный пользователь или приложение пытается получить доступ к зашифрованным файлам или жестким дискам.

Вы можете сгенерировать любой отчет в разделе **Мониторинг и отчеты** → **Отчеты**. Также в разделе **Операции** → **Шифрование и защита данных**, можно создавать следующие отчеты о шифровании:

- Отчет о статусе шифрования запоминающих устройств
- Отчет о правах доступа к зашифрованным дискам
- Отчет об ошибках шифрования файлов

*Чтобы сгенерировать отчет шифрования в разделе **Шифрование и защита данных**:*

1. Убедитесь, что параметр **Показать раздел "Шифрование и защита данных"** в параметрах интерфейса включен.
2. В окне свойств политики выберите вкладку **Настройка событий**.
3. В разделе **Критическое** нажмите **Добавить событие** и установите флажок рядом с событием *Ошибка применения правил шифрования / расшифровки файлов*.
4. Нажмите на кнопку **OK**.

5. В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных**.

6. Откройте один из следующих разделов:

   - **Зашифрованные жесткие диски** – формирует отчет о состоянии шифрования запоминающих устройств или отчет о правах доступа к зашифрованным жестким дискам.

   - **События шифрования** – формирует отчет об ошибках шифрования файлов.

7. 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.

   Если жесткий диск зашифрован с помощью приложения "Лаборатории Касперского", которое не поддерживается Kaspersky Security Center Web Console, используйте Консоль администрирования на основе консоли управления Microsoft Management Console (MMC), чтобы предоставить доступ к диску в автономном режиме.

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.

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.

Просмотр учетных записей и сеансов пользователей

Kaspersky Security Center позволяет управлять учетными записями пользователей и группами учетных записей. Приложение поддерживает два типа учетных записей:

- Учетные записи сотрудников организации. Сервер администрирования получает данные об учетных записях этих пользователей при опросе сети организации.
- Учетные записи внутренних пользователей. Применяются для работы с виртуальными Серверами администрирования. Учетные записи внутренних пользователей создаются и используются только внутри Kaspersky Security Center.

Вы можете просмотреть список учетных записей и сеансов пользователей одним из следующих способов:

- В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы**.
- В главном меню перейдите в раздел **Активы (Устройства)** → **Управляемые устройства** → ссылка <название устройства> → вкладка **Общие** → раздел **Общие** → блок **Сеансы**.

  В разделе **Сеансы** отображаются учетные записи пользователей с активными сеансами на устройствах под управлением Windows.

Список учетных записей и сеансов пользователей отображается правильно, если выполнены следующие требования:

- Используется Агент администрирования той же версии, что и Сервер администрирования, или выше.
- Опрос Active Directory включен для отображения учетных записей пользователей домена.
- На управляемых устройствах под управлением Windows работает служба **Сервера** (**LanmanServer**).

Настройка прав доступа к функциям приложения. Управление доступом на основе ролей

Kaspersky Security Center предоставляет доступ на основе ролей к функциям Kaspersky Security Center и к функциям управляемых приложений "Лаборатории Касперского".

Вы можете настроить права доступа к функциям приложения для пользователей Kaspersky Security Center 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 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	Д
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.	Отсутств

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Д
Общие функции: **Доступ к объектам независимо от их списков ACL**	**Чтение**	Получение доступа Чтение ко всем объектам: **Чтение**.	Отсутствует.	Отсутствует.	Функцио область **функции объекта независи списков** предназн аудита. К пользова предоста право **Чт** функцио области, получают доступ на всем объ Рекоменд предоста права огр кругу пол которым для выпо служебны обязанно Доступ предоста независи прав, даж запреща Чтение к определе объектам
Общие функции: **Базовая функциональность**	• **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с выборками устройств**	• Правила перемещения устройства (создание, изменение или удаление) для виртуального Сервера: **Запись**, **Выполнение операций с выборками устройств**. • Получение мобильного протокола (LWNGT) пользовательского сертификата: **Чтение**. • Установка мобильного протокола (LWNGT) пользовательского сертификата: **Запись**. • Получить список сетей, определенных NLA: **Чтение**. • Добавить, изменить или удалить список сетей, определенных NLA: **Запись**. • Просмотр списка контроля доступа групп: **Чтение**.	• Загрузка обновлений в хранилище Сервера администрирования. • Рассылка отчетов. • Распространение инсталляционных пакетов. • Установка приложений на подчиненные Серверы администрирования.	• Отчет о состоянии защиты. • Отчет об угрозах. • Отчет о наиболее заражаемых устройствах. • Отчет о статусе антивирусных баз. • Отчет об ошибках. • Отчет о сетевых атаках. • Сводный отчет о приложениях для защиты почтовых систем. • Сводный отчет о приложениях для защиты периметра. • Сводный отчет о типах установленных приложений. • Отчет о пользователях зараженных устройств. • Отчет об инцидентах. • Отчет о событиях. • Отчет о работе точек распространения. • Отчет о подчиненных Серверах администрирования. • Отчет о событиях Контроля устройств. • Отчет об уязвимостях.	Отсутств

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Д
		• Просмотрите журнал событий Kaspersky Event Log: **Чтение**. • Просмотр ключа восстановления для восстановления доступа к жесткому диску зашифрованному с помощью BitLocker: **Выполнение**.		• 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.	Отсутств
Общие функции: **Обработка событий**	• **Удалить события** • **Изменить параметры уведомлений о событиях** • **Изменить параметры регистрации событий** • **Запись**	• Изменение параметров регистрации событий: **Изменить параметры регистрации событий**. • Изменение параметров уведомления о событиях: **Изменить параметры уведомлений о событиях**. • Удаление событий: **Удалить события**.	Отсутствует.	Отсутствует.	Параметр • Пара вирус колич обна вирус необ созд вирус • Пара вирус пери оцен обна вирус • Макс колич собы храня базе • Пери собы удале устро
Общие функции: **Операции с Сервером администрирования**	• **Чтение** • **Запись** • **Выполнение** • **Изменение списков управления доступом объектов** • **Выполнение операций с выборками устройств**	• Изменение портов Сервера администрирования для подключения Агента администрирования: **Запись**. • Изменение портов прокси-сервера активации, запущенного на Сервере	• Резервное копирование данных Сервера администрирования. • Обслуживание базы данных.	Отсутствует.	Отсутств

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Д
		администрирования: **Запись**. • Изменение портов прокси-сервера активации для мобильных устройств, запускаемых на Сервере администрирования: **Запись**. • Изменение портов Веб-сервера для распространения автономных пакетов: **Запись**. • Изменение портов Веб-сервера для распространения iOS MDM-профилей: **Запись**. • Изменение SSL-портов Сервера администрирования для подключения с помощью Kaspersky Security Center Web Console: **Запись**. • Изменение портов Сервера администрирования для подключения мобильных устройств: **Запись**. • Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования: **Запись**. • Укажите максимальное количество событий, которое может отправлять Сервер администрирования: **Запись**. • Изменение периода, в течение которого Сервер администрирования может отправлять события: **Запись**.			
Общие функции: **Развертывание приложений "Лаборатории Касперского"**	• **Управление патчами "Лаборатории Касперского"** • **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с выборками устройств**	Одобрить или отклонить установку патча: **Управление патчами "Лаборатории Касперского"**.	Отсутствует.	• Отчет об использовании лицензионных ключей виртуальным Сервером администрирования. • Отчет о версиях приложений "Лаборатории Касперского". • Отчет о несовместимых приложениях.	Инсталля пакет: "Пр "Лаборат Касперск

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Д
				• Отчет о версиях обновлений модулей приложений "Лаборатории Касперского". • Отчет о развертывании защиты.	
Общие функции: **Управление лицензионными ключами**	• **Экспортировать файл ключа** • **Запись**	• Экспорт файл ключа: **Экспортировать файл ключа**. • Изменение параметров лицензионного ключа Сервера администрирования: **Запись**.	Отсутствует.	Отсутствует.	Отсутств
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.	Отсутств

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Д
Общие функции: **Иерархия Серверов администрирования**	**Настроить иерархию Серверов администрирования**	Добавление, обновление или удаление подчиненных Серверов администрирования: **Настроить иерархию Серверов администрирования**.	Отсутствует.	Отсутствует.	Отсутств
Общие функции: **Права пользователей**	**Изменение списков управления доступом объектов**	• Изменение свойств Безопасности любого объекта: **Изменение списков управления доступом объектов**. • Управление ролями пользователей: **Изменение списков управления доступом объектов**. • Управление внутренними пользователями: **Изменение списков управления доступом объектов**. • Управление группами безопасности: **Изменение списков управления доступом объектов**. • Управление псевдонимами: **Изменение списков управления доступом объектов**.	Отсутствует.	Отсутствует.	Отсутств
Общие функции: **Виртуальные Серверы администрирования**	• **Управление виртуальными Серверами** • **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с 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**.	Отсутствует.	Отчет о результатах установки обновлений стороннего ПО.	Отсутств

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Д
		• Перемещение виртуального Сервера администрирования в другую группу: **Управление виртуальными Серверами**. • Установка прав доступа к виртуальному Серверу администрирования: **Управление виртуальными Серверами**.			

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Д
Общие функции: **Управление ключами шифрования**	**Запись**	Импорт ключей шифрования: **Запись**.	Отсутствует.	Отсутствует.	Отсутств
Управление мобильными устройствами: Основные	• **Подключение новых устройств** • **Отправка только информационных команд на мобильные устройства** • **Отправка команд на мобильные устройства** • **Управление сертификатами** • **Чтение** • **Запись**	• Получение восстановленных данных службы управления ключами: **Чтение**. • Удаление сертификатов пользователей: **Управление сертификатами**. • Получение публичной части сертификата пользователя: **Чтение**. • Проверка, включена ли инфраструктура открытых ключей: **Чтение**. • Проверка учетной записи инфраструктуры открытых ключей: **Чтение**. • Получение шаблонов инфраструктуры открытых ключей: **Чтение**. • Получение шаблонов инфраструктуры открытых ключей с помощью расширенного использования ключа (EKU) сертификата: **Чтение**. • Проверка, не отозван ли сертификат инфраструктуры открытых ключей: **Чтение**. • Обновление параметров выпуска сертификатов пользователя: **Управление сертификатами**. • Получение параметров выпуска сертификатов пользователя: **Чтение**. • Получение пакетов по названию и версиям приложений: **Чтение**. • Установка или отмена сертификатов пользователя: **Управление сертификатами**.	Отсутствует.	Отсутствует.	Отсутств

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Д
		• Обновление сертификата пользователя: **Управление сертификатами**. • Установка тега для сертификата пользователя: **Управление сертификатами**. • Запуск генерации инсталляционного пакета, содержащего iOS MDM-профиль; отмена генерации инсталляционного пакета, содержащего iOS MDM-профиль: **Подключение новых устройств**.			
Управление системой: Подключения	• **Запуск RDP-сессий** • **Подключение к существующим RDP-сессиям** • **Создание туннелирования** • **Сохранение файлов с устройств на рабочем месте администратора** • **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с выборками устройств**	• Создание сеанса совместного доступа к рабочему столу: **Запуск RDP-сессий**. • Создание RDP-сеанса: **Подключение к существующим RDP-сессиям**. • Создание туннеля: **Создание туннелирования**. • Сохранение списка сетей: **Сохранение файлов с устройств на рабочем месте администратора**.	Отсутствует.	Отчет о пользователях устройства.	Отсутств
Управление системой: Инвентаризация оборудования	• **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с выборками устройств**	• Получение или экспорт объектов инвентаризации оборудования: **Чтение**. • Добавление, настройка или удаление объектов инвентаризации оборудования: **Запись**.	Отсутствует.	• Отчет о реестре оборудования. • Отчет об изменении конфигурации. • Отчет об оборудовании.	Отсутств
Управление системой: Network Access Control	• **Чтение** • **Запись**	• Просмотр параметров Cisco: **Чтение**. • Изменение параметров Cisco: **Запись**.	Отсутствует.	Отсутствует.	Отсутств
Управление системой: Развертывание операционной системы	• **Развертывание PXE-серверов** • **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с выборками устройств**	• Развертывание PXE-серверов: **Развертывание PXE-серверов**. • Просмотр списка PXE-серверов: **Чтение**.	Создание инсталляционного пакета на основе образа ОС эталонного устройства.	Отсутствует.	Инсталля пакет: Об операцио системы.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Д
		• Запуск или остановка процесс установки на PXE-клиентах: **Выполнение**. • Управление драйверами для среды WinPE и образов операционной системы: **Запись**.			
Управление системой: Системное администрирование	• **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с 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. • Закрытие уязвимостей. • Установка требуемых обновлений и закрытия уязвимостей.	Отчет об обновлениях ПО.	Отсутств
Управление системой: Удаленная установка	• **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с выборками устройств**	• Просмотр Системного администрирования стороннего производителя на основе свойств инсталляционного пакета: **Чтение**. • Изменение Системного администрирования на основе свойств инсталляционного пакета: **Запись**.	Отсутствует.	Отсутствует.	Инсталля пакеты: • Поль прил • Паке
Управление системой: Инвентаризация приложений	• **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с 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.	Отсутств
Управление системой: Удаленное выполнение скриптов	• **Чтение** • **Запись** • **Выполнение** • **Выполнение операций с выборками устройств**	Пользователь может просматривать свойства задачи: **Чтение**.	"Удаленное выполнение скриптов"	Отсутствует.	Отсутств

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Д
		Пользователь может создать, удалить или изменить инсталляционный пакет: **Запись**. Пользователь может запустить задачу: **Запись**. На клиентских устройствах с операционной системой Linux скрипты выполняются с правами root. Пользователь может запустить задачу или запланировать ее запуск: **Выполнение**. Пользователь может запустить задачу на выбранных устройствах: **Выполнение операций с выборками устройств**.			

Предопределенные роли пользователей

Роли пользователей, назначенные пользователям Kaspersky Security Center, предоставляют им набор прав доступа к функциям приложения.

Пользователям, которые были созданы на виртуальном Сервере, невозможно назначить роли на Сервере администрирования.

Вы можете использовать предопределенные роли пользователей с уже настроенным набором прав или создавать роли. При создании роли вам нужно задать область действия и назначить права доступа к функциям Kaspersky Security Center. Некоторые из предопределенных ролей пользователей, доступных в Kaspersky Security Center, могут быть связаны с определенными должностями, например, **Аудитор**, **Специалист по безопасности**, **Контролер** (эти роли присутствуют в Kaspersky Security Center 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 функциональной области **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 области **Общие функции: Базовая функциональность**.

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.
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**: функциональная область **Управление отчетами**. Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации.
Администратор Системного администрирования	Разрешает все операции в области **Общие функции**: **Базовая функциональность** и **Управление системой** (включая все функции).
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:
   - **Активы (Устройства)** → **Иерархия групп**.
   - **Активы (Устройства)** → **Задачи**.
   - **Мониторинг и отчеты** → **Отчеты**.
   - **Активы (Устройства)** → **Выборки устройств**.
   - **Мониторинг и отчеты** → **Выборки событий**.
2. Откройте свойства объекта, к которому вы хотите настроить права доступа.

   Чтобы открыть окно свойств группы администрирования или задачи, нажмите на название объекта. Свойства других объектов можно открыть с помощью кнопки в панели инструментов.
3. В окне свойств откройте раздел **Права доступа**.

   Откроется список пользователей. Перечисленные пользователи и группы безопасности имеют права доступа к объекту. Если вы используете иерархию групп администрирования или Серверов, список и права доступа по умолчанию наследуются от родительской группы администрирования или главного Сервера.
4. Чтобы иметь возможность изменять список, включите параметр **Использовать права пользователей**.
5. Настройте права доступа:
   - Используйте кнопки **Добавить** и **Удалить** для изменения списка.
   - Укажите права доступа для пользователя или группы безопасности. Выполните одно из следующих действий:
     - Если вы хотите указать права доступа вручную, выберите пользователя или группу безопасности, нажмите на кнопку **Права доступа** и укажите права доступа.
     - Если вы хотите назначить пользовательскую роль пользователю или группе безопасности, 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 меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Права доступа** установите флажок рядом с именем пользователя или группы безопасности, которым нужно назначить права, а затем нажмите на кнопку **Права доступа**.

   Вы не можете выбрать несколько пользователей или групп безопасности одновременно. Если вы выберете более одного объекта, кнопка **Права доступа** будет неактивна.

3. Настройте набор прав для пользователя или группы:

   a. Разверните узел с функциями Сервера администрирования или другого приложения "Лаборатории Касперского".

   b. Установите флажок **Разрешить** или **Запретить** рядом с нужной функцией или правом доступа.

      Пример 1: Установите флажок **Разрешить** рядом с узлом **Интеграции приложения**, чтобы предоставить пользователю или группе все доступные права доступа к функции интеграции приложения (**Чтение**, **Запись** и **Выполнение**).

      Пример 2: Разверните узел **Управление ключами шифрования** и установите флажок **Разрешить** рядом с разрешением **Запись**, чтобы предоставить пользователю или группе право доступа на **Запись** к функции управления ключами шифрования.

4. После настройки набора прав доступа нажмите на кнопку **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 операционной системы
    - Системное администрирование
    - Удаленная установка
    - Инвентаризация приложений

Если для права не выбрано ни **Разрешить**, ни **Запретить**, оно считается *неопределенным*: право отклоняется до тех пор, пока оно не будет явно отклонено или разрешено для пользователя.

Права пользователей являются суммой следующего:

- собственных прав пользователя;
- прав всех ролей, назначенных пользователю;
- прав всех групп безопасности, в которые входит пользователь;
- прав всех ролей, назначенных группам, в которые входит пользователь.

Если хотя бы в одном наборе прав есть запрещенное право (для права установлен флажок **Запретить**), тогда для пользователя это право запрещено, даже если в других наборах прав оно разрешено или не определено.

Также вы можете добавить пользователей и группы безопасности в область пользовательской роли, чтобы использовать различные возможности Сервера администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

Добавление учетной записи внутреннего пользователя

Если вы хотите добавить учетную запись пользователя, убедитесь, что у вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области Общие функции: Права пользователей.

Чтобы добавить новую учетную запись пользователя Kaspersky Security Center:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Добавить пользователя** укажите параметры нового пользователя:
   - **Имя**
   - **Пароль**

     Пароль должен соответствовать следующим правилам:
     - Длина пароля должна быть от 8 до 256 символов.
     - Пароль должен содержать символы как минимум трех групп из списка ниже:
       - верхний регистр (A–Z);
       - нижний регистр (a–z);
       - числа (0–9);
       - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
     - Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", если "." расположена перед "@".

     Чтобы посмотреть введенный пароль, нажмите на кнопку .

     Вы можете включить параметр **Пользователю надо сменить пароль при первом входе**, чтобы принудительно изменить пароль при первой аутентификации пользователя.
4. Сохраните изменения для завершения создания учетной записи пользователя.

Учетная запись пользователей добавлена в список пользователей.

Чтобы войти в систему с помощью созданной учетной записи внутреннего пользователя на консоли OSMP, требуется назначить роль для этой учетной записи. Прежде чем войти в приложение убедитесь, что у внутренней учетной записи пользователя есть роль. В противном случае произойдет ошибка входа в систему.

Создание группы безопасности

Чтобы создать группу безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Группы**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Создать группу безопасности** укажите следующие параметры новой группы безопасности:
   - **Имя группы**
   - **Описание**
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Группа безопасности добавлена в список групп.

Изменение учетной записи внутреннего пользователя

Если вы хотите изменить учетную запись пользователя, убедитесь, что у вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области Общие функции: Права пользователей.

Чтобы изменить учетную запись внутреннего пользователя Kaspersky Security Center:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Выберите учетную запись пользователя, которую требуется изменить.
3. В открывшемся окне на вкладке **Общие** измените параметры учетной записи пользователя:
   - **Статус пользователя**

     При необходимости переведите переключатель в положение **Выключено**, чтобы запретить пользователю подключаться к приложению. Например, можно отключить учетную запись после того, как сотрудник увольняется из компании.
   - **Имя**
   - **Полное имя**
   - **Описание**
   - **Адрес электронной почты**
   - **Основной телефон**

- **Пароль**

  При необходимости вы можете установить новый пароль для подключения пользователя к Kaspersky Security Center следующим образом:

  a. Нажмите на кнопку **Изменение пароля** и установите новый пароль для учетной записи пользователя.

  Пароль должен соответствовать следующим правилам:

  - Длина пароля должна быть от 8 до 256 символов.
  - Пароль должен содержать символы как минимум трех групп из списка ниже:
    - верхний регистр (A–Z);
    - нижний регистр (a–z);
    - числа (0–9);
    - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
  - Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", если "." расположена перед "@".

  Чтобы посмотреть введенный пароль, нажмите на кнопку .

  b. При необходимости включите параметр **Пользователю надо сменить пароль при первом входе**, чтобы принудительно изменить пароль при следующей аутентификации пользователя.

  c. Если учетная запись пользователя защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите учетные данные учетной записи, у которой есть право Изменение списков управления доступом объектов в функциональной области Общие функции: Права пользователей.

4. На вкладке **Дополнительные настройки безопасности** вы можете указать параметры безопасности для этой учетной записи.

5. На вкладке **Группы** можно добавить пользователя или группу безопасности.

6. На вкладке **Устройства** можно назначить устройства пользователю.

7. На вкладке **Роли** можно назначить роль пользователю.

8. Сохраните изменения для завершения изменения учетной записи пользователя.

Измененная учетная запись пользователя отобразится в списке пользователей.

Изменение группы безопасности

Чтобы изменить группу безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Группы**.
2. Выберите группу безопасности, которую требуется изменить.
3. В открывшемся окне измените параметры группы безопасности:
   - На вкладке **Общие** можно изменить параметры **Имя** и **Описание**. Эти параметры доступны только для внутренних групп безопасности.
   - На вкладке **Пользователи** можно добавить пользователей в группу безопасности. Эти параметры доступны только для внутренних пользователей и внутренних групп безопасности.
   - На вкладке **Роли** можно назначить роль группе безопасности.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Изменения применены к группе безопасности.

Назначение роли пользователю или группе безопасности

Чтобы назначить роли пользователю или группе безопасности:

1. В главном окне приложения перейдите в раздел 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 инструкциям мастера: выберите роль, которую вы хотите назначить выбранным пользователям или группам безопасности, а затем выберите область применения роли.

   Область роли пользователя – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

В результате роль с набором прав для работы с Сервером администрирования будет назначена пользователю (или пользователям, или группе безопасности). В списке пользователей или групп безопасности отображается флажок в столбце **Имеет назначенные роли**.

Пользователям, которые были созданы на виртуальном Сервере, невозможно назначить роли на Сервере администрирования.

Добавление учетных записей пользователей во внутреннюю группу безопасности

Учетные записи внутренних пользователей можно добавлять только во внутреннюю группу безопасности.

Чтобы добавить учетные записи пользователей в группу безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Установите флажки напротив учетных записей пользователей, которые требуется добавить в группу безопасности.
3. Нажмите на кнопку **Назначить группу**.
4. В открывшемся окне **Назначить группу** выберите группу безопасности, в которую требуется добавить учетные записи пользователей.
5. Нажмите на кнопку **Сохранить**.

Учетные записи пользователей добавлены в группу безопасности. Также можно добавить внутренних пользователей в группу безопасности, используя параметры группы.

Назначение пользователя владельцем устройства

Информацию о назначении пользователя владельцем мобильного устройства см. в справке Kaspersky Secure Mobility Management.

Чтобы назначить пользователя владельцем устройства:

1. Если вы хотите назначить владельца устройства, подключенного к виртуальному Серверу администрирования, сначала переключитесь на виртуальный Сервер администрирования:
   a. В главном меню нажмите на значок шеврона (›) справа от текущего имени Сервера администрирования.
   b. Выберите требуемый Сервер администрирования.
2. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.

   Откроется список пользователей. Если вы в данный момент подключены к виртуальному Серверу администрирования, в список входят пользователи текущего виртуального Сервера администрирования и главного Сервера администрирования.
3. Нажмите на учетную запись пользователя, которую требуется назначить в качестве владельца устройству.

4. В открывшемся окне свойств пользователя выберите вкладку **Устройства**.

5. Нажмите на кнопку **Добавить**.

6. Из списка устройств выберите устройство, которое вы хотите назначить пользователю.

7. Нажмите на кнопку **ОК**.

Выбранное устройство добавляется в список устройств, назначенных пользователю.

Также можно выполнить эту операцию в группе **Активы (Устройства)** → **Управляемые устройства**, выбрав имя устройства, которое вы хотите назначить, и перейдя по ссылке **Сменить владельца устройства**.

Настройка двухфакторной аутентификации для всех пользователей

В этом сценарии описывается, как включить двухфакторную аутентификацию для всех пользователей и как исключить учетные записи пользователей из двухфакторной аутентификации. Если вы не включили двухэтапную проверку для своей учетной записи, прежде чем включить ее для других пользователей, приложение сначала откроет окно включения двухэтапной проверки для вашей учетной записи. В этом сценарии также описано, как включить двухэтапную проверку для вашей учетной записи.

Если вы включили двухэтапную проверку для своей учетной записи, вы можете перейти к включению двухэтапной проверки для всех пользователей.

Предварительные требования

Прежде чем начать:

- Убедитесь, что ваша учетная запись имеет право Изменение списков управления доступом объектов в функциональной области **Общие функции: Права пользователей** для изменения параметров безопасности учетных записей других пользователей.
- Убедитесь, что другие пользователи Сервера администрирования установили на свои устройства приложение для аутентификации.

Этапы

Включение двухэтапной проверки для всех пользователей состоит из следующих этапов:

1. **Установка приложения для аутентификации на устройство**

   Вы можете установить любое приложение для аутентификации, которое поддерживает алгоритм формирования одноразового пароля на основе времени (TOTP).

Доступно в России:

- Kaspersky Password Manager для бизнеса (рекомендуется)
- Bitrix24 OTP
- Yandex ID
- Avanpost Authenticator
- Aladdin 2FA
- Рутокен OTP

Доступно во всем мире (включая Россию):

- Google Authenticator
- Microsoft Authenticator

Чтобы проверить, поддерживает ли Kaspersky Security Center приложение для аутентификации, которое вы хотите использовать, включите двухфакторную аутентификацию для всех пользователей или для определенного пользователя.

Один из шагов предполагает, что вы указываете код безопасности, сгенерированный приложением для аутентификации. Если проверка проходит успешно, значит Kaspersky Security Center поддерживает выбранное приложение для аутентификации.

> Категорически не рекомендуется устанавливать приложение для аутентификации на том же устройстве, с которого выполняется подключение к Серверу администрирования.

2. **Синхронизация времени приложения для аутентификации и времени устройства, на котором установлен Сервер администрирования**

   Убедитесь, что время на устройстве с приложением для аутентификации и время на устройстве с Сервером администрирования синхронизированы с UTC с помощью внешних источников времени. Иначе возможны сбои при аутентификации и активации двухэтапной проверки.

3. **Включение двухэтапной проверки и получение секретного ключа для своей учетной записи**

   Инструкции:

   - Для Консоли администрирования на основе MMC: Включение двухфакторной аутентификации для вашей учетной записи.
   - Для Web Console: Включение двухэтапной проверки для вашей учетной записи.

   После включения двухэтапной проверки для своей учетной записи вы можете включить двухэтапную проверку для всех пользователей.

4. **Включение двухфакторной аутентификации для всех пользователей**

   Пользователи с включенной двухэтапной проверкой должны использовать ее для входа на Сервер администрирования.

Инструкции:

- Для Консоли администрирования на основе MMC: Включение двухфакторной аутентификации для всех пользователей.
- Для Web Console: Включение двухэтапной проверки для всех пользователей.

5. **Изменение имени издателя кода безопасности**

   Если у вас несколько Серверов администрирования с похожими именами, возможно, вам придется изменить имена издателей кода безопасности для лучшего распознавания разных Серверов администрирования.

   Инструкции:

   - Для Консоли администрирования на основе MMC: Изменение имени издателя кода безопасности.
   - Для Web Console: Изменение имени издателя кода безопасности.

6. **Исключение учетных записей пользователей, для которых не требуется включать двухфакторную аутентификацию**

   При необходимости исключите учетные записи пользователей из двухфакторной аутентификации. Пользователям с исключенными учетными записями не нужно использовать двухфакторную аутентификацию для входа на Сервер администрирования.

   Инструкции:

   - Для Консоли администрирования на основе MMC: Исключение учетных записей из двухфакторной аутентификации.
   - Для Web Console: Исключение учетных записей из двухэтапной проверки.

7. **Настройка двухэтапной проверки для вашей учетной записи**

   Если пользователи не исключены из двухфакторной аутентификации и двухфакторная аутентификация еще не настроена для их учетных записей, им необходимо настроить ее в окне, открывающемся при входе в Kaspersky Security Center. Иначе они не смогут получить доступ к Серверу администрирования в соответствии со своими правами.

   Инструкции:

   - Для Консоли администрирования на основе MMC: Настройка двухфакторной аутентификации для вашей учетной записи.
   - Для Web Console: Настройка двухэтапной проверки для вашей учетной записи.

Результаты

После выполнения этого сценария:

- Двухфакторная аутентификация для вашей учетной записи включена.
- Двухэтапная проверка включена для всех учетных записей пользователей Сервера администрирования, кроме исключенных учетных записей пользователей.

О двухфакторной аутентификации

Если для учетной записи включена двухфакторная аутентификация, для входа в Консоль администрирования или Kaspersky Security Center Web Console требуется одноразовый код безопасности, помимо имени пользователя и пароля. Если доменная аутентификация включена, пользователю достаточно ввести одноразовый код безопасности.

Чтобы использовать двухфакторную аутентификацию, установите на мобильное устройство или компьютер приложение для аутентификации, которое генерирует одноразовые коды безопасности. Вы можете использовать любое приложение для аутентификации, которое поддерживает алгоритм формирования одноразового пароля на основе времени (TOTP).

Доступно в России:

- Kaspersky Password Manager для бизнеса (рекомендуется)
- Bitrix24 OTP
- Yandex ID
- Avanpost Authenticator
- Aladdin 2FA
- Рутокен OTP

Доступно во всем мире (включая Россию):

- Google Authenticator
- Microsoft Authenticator

Чтобы проверить, поддерживает ли Kaspersky Security Center приложение для аутентификации, которое вы хотите использовать, включите двухфакторную аутентификацию для всех пользователей или для определенного пользователя.

Один из шагов предполагает, что вы указываете код безопасности, сгенерированный приложением для аутентификации. Если проверка проходит успешно, значит Kaspersky Security Center поддерживает выбранное приложение для аутентификации.

> Настоятельно рекомендуется сохранить секретный ключ или QR-код и хранить его в надежном месте. Это поможет вам восстановить доступ к Kaspersky Security Center Web Console в случае потери доступа к мобильному устройству.

Чтобы обезопасить использование Kaspersky Security Center, вы можете включить двухфакторную аутентификацию для своей учетной записи и включить двухфакторную аутентификацию для всех пользователей.

> Вы можете исключить учетные записи из двухфакторной аутентификации. Это может быть необходимо для служебных учетных записей, которые не могут получить защитный код для аутентификации.

Правила и ограничения

Чтобы иметь возможность активировать двухфакторную аутентификацию для всех пользователей и деактивировать двухфакторную аутентификацию для отдельных пользователей:

- Убедитесь, что у вашей учетной записи есть право Изменение списков управления доступом к объектам в функциональной области **Общие функции: Права пользователя**.
- Включите двухфакторную аутентификацию для вашей учетной записи.

Чтобы выключить двухфакторную аутентификацию для всех пользователей:

- Убедитесь, что у вашей учетной записи есть право Изменение списков управления доступом к объектам в функциональной области **Общие функции: Права пользователя**.
- Войдите в Kaspersky Security Center Web Console с помощью двухфакторной аутентификации.

Если для учетной записи на Сервере администрирования Kaspersky Security Center версии 13 или выше включена двухфакторная аутентификация, то пользователь не сможет войти в приложение Kaspersky Security Center Web Console версий 12, 12.1 или 12.2.

Перевыпуск секретного ключа

Любой пользователь может повторно выпустить секретный ключ, используемый для двухфакторной аутентификации. Когда пользователь входит на Сервер администрирования с перевыпущенным секретным ключом, новый секретный ключ сохраняется для учетной записи пользователя. Если пользователь неправильно вводит новый секретный ключ, новый секретный ключ не сохраняется, а текущий секретный ключ остается действительным.

Код безопасности имеет идентификатор, называемый также *имя издателя*. Имя издателя кода безопасности используется в качестве идентификатора Сервера администрирования в приложении для аутентификации. Имя издателя кода безопасности имеет значение по умолчанию, такое же, как имя Сервера администрирования. Вы можете изменить имя издателя кода безопасности. Если вы изменили имя издателя кода безопасности, необходимо выпустить новый секретный ключ и передать его приложению для аутентификации.

Включение двухфакторной аутентификации для вашей учетной записи (Web Console)

Вы можете включить двухфакторную аутентификацию только для своей учетной записи.

Перед тем как включить двухфакторную аутентификацию для своей учетной записи, убедитесь, что на мобильном устройстве установлено приложение для аутентификации. Убедитесь, что время, установленное в приложении для аутентификации, синхронизировано со временем устройства, на котором установлен Сервер администрирования.

Чтобы включить двухфакторную аутентификацию для учетной записи пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Нажмите на имя вашей учетной записи.

3. В открывшемся окне свойств пользователя выберите вкладку **Дополнительные настройки безопасности**.

4. На вкладке **Дополнительные настройки безопасности**:

   a. Выберите параметр **Запрашивать только имя пользователя, пароль и код безопасности (двухэтапная проверка)**. Нажмите на кнопку **Сохранить**.

   b. В открывшемся окне двухфакторной аутентификации нажмите **Узнайте, как настроить двухэтапную проверку**.

   Введите секретный ключ в приложении для аутентификации или нажмите **Просмотреть QR-код** и отсканируйте QR-код с помощью приложения для аутентификации на мобильном устройстве, чтобы получить одноразовый код безопасности.

   c. В окне двухфакторной аутентификации укажите код безопасности, сгенерированный приложением для аутентификации и нажмите на кнопку **Проверить и применить**.

5. Нажмите на кнопку **Сохранить**.

Двухфакторная аутентификация для вашей учетной записи включена.

Включение двухфакторной аутентификации для вашей учетной записи (на базе MMC)

Перед тем как включить двухфакторную аутентификацию для своей учетной записи, убедитесь, что на мобильном устройстве установлено приложение для аутентификации. Убедитесь, что время, установленное в приложении для аутентификации, синхронизировано со временем Сервера администрирования.

Чтобы включить двухфакторную аутентификацию для учетной записи:

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.

2. В окне свойств Сервера администрирования в панели **Разделы** перейдите в раздел **Дополнительно**, а затем **Двухэтапная проверка**.

3. В разделе **Двухэтапная проверка** нажмите на кнопку **Настроить**.

   Если для вашей учетной записи уже включена двухфакторная аутентификация, при нажатии на кнопку **Настроить** сбрасывается секретный ключ, чтобы можно было перенастроить двухфакторную аутентификацию.

   В открывшемся окне свойств двухфакторной аутентификации отображается секретный ключ.

4. Введите секретный ключ в приложение для аутентификации, чтобы получить одноразовый код безопасности. Вы можете указать секретный ключ в приложении для аутентификации вручную или отсканировать QR-код с помощью приложения для аутентификации на мобильном устройстве.

5. Укажите код безопасности, сгенерированный приложением для аутентификации, а затем нажмите на кнопку **OK**, чтобы закрыть окно свойств двухфакторной аутентификации.

6. Нажмите на кнопку **Применить**.

7. Нажмите на кнопку **ОК**.

двухфакторная аутентификация для вашей учетной записи включена.

Включение обязательной двухфакторной аутентификации для всех пользователей (Web Console)

Вы можете включить двухфакторную аутентификацию для всех пользователей Сервера администрирования, если у вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области **Общие функции: Права пользователей** и если вы выполнили аутентификацию с помощью двухфакторной аутентификации.

Чтобы включить двухфакторную аутентификацию для всех пользователей:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Дополнительные настройки безопасности** окна свойств включите **двухфакторную аутентификацию для всех пользователей**.

3. Если вы не включили двухфакторную аутентификацию для своей учетной записи, приложение откроет окно включения двухфакторной аутентификации для вашей учетной записи.

   a. В открывшемся окне двухфакторной аутентификации нажмите **Узнайте, как настроить двухэтапную проверку**.

   b. Введите секретный ключ вручную в приложении для аутентификации или нажмите **Просмотреть QR-код** и отсканируйте QR-код с помощью приложения для аутентификации на мобильном устройстве, чтобы получить одноразовый код безопасности.

   c. В окне двухфакторной аутентификации укажите код безопасности, сгенерированный приложением для аутентификации и нажмите на кнопку **Проверить и применить**.

Двухфакторная аутентификация для всех пользователей включена. Пользователям Сервера администрирования, включая пользователей, которые были добавлены после включения двухфакторной аутентификации для всех пользователей, необходимо настроить двухфакторную аутентификацию для своих учетных записей, за исключением пользователей, учетные записи которых исключены из двухфакторной аутентификации.

Включение двухфакторной аутентификации для всех пользователей (на базе MMC)

Вы можете включить двухфакторную аутентификацию для всех пользователей Сервера администрирования, если у вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области **Общие функции: Права пользователей** и если вы выполнили аутентификацию с помощью двухфакторной аутентификации.

Чтобы включить двухфакторную аутентификацию для всех пользователей:

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.

2. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Дополнительно**, а затем **Двухэтапная проверка**.

3. Нажмите на кнопку **Установить как обязательную**, чтобы включить двухфакторную аутентификацию для всех пользователей.

4. Если вы не включили двухфакторную аутентификацию для своей учетной записи, приложение откроет окно включения двухфакторной аутентификации для вашей учетной записи.

   a. Введите секретный ключ в приложение для аутентификации, чтобы получить одноразовый код безопасности. Введите секретный ключ вручную в приложении для аутентификации или отсканируйте QR-код с помощью приложения для аутентификации на мобильном устройстве, чтобы получить одноразовый код безопасности.

   b. Укажите код безопасности, сгенерированный приложением для аутентификации, а затем нажмите на кнопку **ОК**, чтобы закрыть окно свойств двухфакторной аутентификации.

5. В разделе **Двухэтапная проверка** нажмите на кнопку **Применить** и нажмите на кнопку **ОК**.

Двухфакторная аутентификация для всех пользователей включена. Пользователям Сервера администрирования, включая пользователей, которые были добавлены после включения этого параметра, необходимо настроить двухфакторную аутентификацию для своих учетных записей, за исключением пользователей, учетные записи которых исключены из двухфакторной аутентификации.

Выключение двухфакторной аутентификации для учетной записи пользователя (Web Console)

Вы можете выключить двухфакторную аутентификацию для своей учетной записи, а также для учетной записи любого другого пользователя.

Вы можете выключить двухфакторную аутентификацию для другой учетной записи пользователя, если у вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области **Общие функции: Права пользователей** и если вы выполнили аутентификацию с помощью двухфакторной аутентификации.

Чтобы выключить двухфакторную аутентификацию для учетной записи пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли → Пользователи**.

2. Нажмите на учетную запись внутреннего пользователя, для которой вы хотите выключить двухфакторную аутентификацию. Это может быть ваша собственная учетная запись или учетная запись любого другого пользователя.

3. В открывшемся окне свойств пользователя выберите вкладку **Защита учетной записи**.

4. На вкладке **Защита учетной записи** выберите параметр **Запрашивать только имя пользователя и пароль**, если вы хотите выключить двухфакторную аутентификацию для учетной записи пользователя.

5. Нажмите на кнопку **Сохранить**.

Двухфакторная аутентификация для вашей учетной записи выключена.

Если вы хотите восстановить доступ пользователя, который не может войти в Kaspersky Security Center Web Console с помощью двухфакторной аутентификации, выключите двухфакторную аутентификацию для этой учетной записи пользователя и выберите параметр **Запрашивать только имя пользователя и пароль** как описано выше. После этого войдите в Kaspersky Security Center Web Console под учетной записью пользователя, для которого вы выключили двухфакторную аутентификацию, и снова включите аутентификацию.

Выключение двухфакторной аутентификации для учетной записи пользователя (на базе MMC)

Чтобы выключить двухфакторную аутентификацию для вашей учетной записи:

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Дополнительно**, а затем **Двухэтапная проверка**.
3. В разделе **Двухэтапная проверка** нажмите на кнопку **Выключить**.
4. Нажмите на кнопку **Применить**.
5. Нажмите на кнопку **OK**.

Двухфакторная аутентификация для вашей учетной записи выключена.

Вы можете выключить двухфакторную аутентификацию для других учетных записей пользователей. Эта защита используется, например, если пользователь потеряет или сломает мобильное устройство.

Вы можете выключить двухфакторную аутентификацию для другой учетной записи пользователя, только если у вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области **Общие функции: Права пользователей** и если вы выполнили аутентификацию с помощью двухфакторной аутентификации. Следуя приведенным ниже инструкциям, вы также можете выключить двухфакторную аутентификацию для своей учетной записи.

Чтобы выключить двухфакторную аутентификацию для учетной записи любого пользователя:

1. В дереве консоли откройте папку **Учетные записи пользователей**.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.
2. В рабочей области папки нажмите на учетную запись пользователя, для которой вы хотите выключить двухфакторную аутентификацию.

   Для всех учетных записей пользователей, для которых включена двухэтапная проверка, в столбце **Требуется 2FA** установите значение **Да**.
3. В окне **Свойства: <Имя пользователя>** выберите раздел **Двухэтапная проверка**.

4. В разделе **Двухэтапная проверка** выберите следующие параметры:

   - Если вы хотите выключить двухфакторную аутентификацию для выбранной учетной записи пользователя, нажмите на кнопку **Выключить**.

   - Если вы хотите исключить эту учетную запись пользователя из двухфакторной аутентификации, выберите параметр **Пользователь может пройти аутентификацию, используя только имя пользователя и пароль**.

5. Нажмите на кнопку **Применить**.

6. Нажмите на кнопку **OK**.

Двухфакторная аутентификация учетной записи пользователя выключена.

Если вы хотите восстановить доступ пользователя, который не может войти в Консоль администрирования с помощью двухфакторной аутентификации, выключите двухфакторную аутентификацию для этой учетной записи пользователя и выберите параметр **Пользователь может пройти аутентификацию, используя только имя пользователя и пароль** в разделе **Двухэтапная проверка**, как описано выше. После этого войдите в Консоль администрирования под учетной записью пользователя, для которого вы выключили двухфакторную аутентификацию, и снова включите проверку.

Выключение обязательной двухфакторной аутентификации для всех пользователей (Web Console)

Вы можете выключить обязательную двухфакторную аутентификацию для всех пользователей, если двухфакторная аутентификация включена для вашей учетной записи и у вашей учетной записи есть право Изменение списков ACL объекта в разделе **Общие функции: Права пользователей**. Если двухфакторная аутентификация не включена для вашей учетной записи, вам нужно включить двухфакторную аутентификацию для своей учетной записи, прежде чем выключить ее для всех пользователей.

Чтобы выключить двухфакторную аутентификацию для всех пользователей:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Дополнительные настройки безопасности** окна свойств выключите переключатель **двухфакторной аутентификации для всех пользователей**.

Двухфакторная аутентификация для всех пользователей выключена. Выключение двухфакторной аутентификации для всех пользователей не применяется к конкретным учетным записям, для которых двухфакторная аутентификация ранее была включена отдельно.

Выключение обязательной двухфакторной аутентификации для всех пользователей (на базе MMC)

Вы можете выключить обязательную двухфакторную аутентификацию для всех пользователей Сервера администрирования, если у вас есть право Изменение списков управления доступом объектов в функциональной области **Общие функции: Права пользователей** и если вы выполнили аутентификацию с помощью двухфакторной аутентификации.

Чтобы выключить двухфакторную аутентификацию для всех пользователей:

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Дополнительно**, а затем **Двухэтапная проверка**.
3. Нажмите на кнопку **Установить как необязательную**, чтобы выключить двухфакторную аутентификацию для всех пользователей.
4. Нажмите на кнопку **Применить** в разделе **Двухэтапная проверка**.
5. Нажмите на кнопку **ОК** в разделе **Двухэтапная проверка**.

Двухфакторная аутентификация для всех пользователей выключена. Выключение двухфакторной аутентификации для всех пользователей не применяется к конкретным учетным записям, для которых двухфакторная аутентификация ранее была включена отдельно.

Исключение учетных записей из двухфакторной аутентификации (Web Console)

Вы можете исключить учетные записи пользователей из двухфакторной аутентификации, если у вас есть право Изменение списков ACL объекта в функциональной области **Общие функции: Права пользователей**.

Если учетная запись пользователя исключена из списка двухфакторной аутентификации для всех пользователей, этому пользователю не нужно использовать двухфакторную аутентификацию.

Исключение учетных записей из двухфакторной аутентификации может быть необходимо для служебных учетных записей, которые не могут передать код безопасности во время аутентификации.

Если вы хотите исключить некоторые учетные записи пользователей из двухфакторной аутентификации:

1. Вам нужно выполнить опрос контроллера домена Microsoft Active Directory, чтобы обновить список пользователей Сервера администрирования, если вы хотите исключить учетные записи Active Directory.
2. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
3. На вкладке **Дополнительные настройки безопасности** окна свойств в таблице исключений для двухфакторной аутентификации нажмите на кнопку **Добавить**.

4. В открывшемся окне:

   a. Выберите учетную запись пользователя, которую вы хотите исключить.

   b. Нажмите на кнопку **OK**.

Выбранные учетные записи пользователей исключены из двухфакторной аутентификации.

Исключение учетных записей из двухфакторной аутентификации (на базе MMC)

Вы можете исключить учетную запись из двухфакторной аутентификации, если у вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области **Общие функции: Права пользователей**.

Если учетная запись пользователя исключена из двухфакторной аутентификации, этот пользователь может войти в Консоль администрирования или Kaspersky Security Center Web Console без использования двухфакторной аутентификации.

Исключение учетных записей из двухфакторной аутентификации может быть необходимо для служебных учетных записей, которые не могут передать код безопасности во время аутентификации.

Чтобы исключить учетную запись пользователя из двухфакторной аутентификации:

1. Если вы хотите исключить учетную запись Active Directory, выполните опрос Active Directory, чтобы обновить список пользователей Сервера администрирования.

2. В дереве консоли откройте папку **Учетные записи пользователей**.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

3. В рабочей области папки нажмите на учетную запись пользователя, которую вы хотите исключить из двухфакторной аутентификации.

4. В окне **Свойства: <Имя пользователя>** выберите раздел **Двухэтапная проверка**.

5. В открывшемся разделе выберите параметр **Пользователь может пройти аутентификацию, используя только имя пользователя и пароль**.

6. В разделе **Двухэтапная проверка** нажмите на кнопку **Применить** и нажмите на кнопку **OK**.

Эта учетная запись пользователя исключена из двухфакторной аутентификации. Вы можете проверить исключенные учетные записи в списке учетных записей пользователей.

Изменение имени издателя кода безопасности (Web Console)

У вас может быть несколько идентификаторов (также их называют издателями) для разных Серверов администрирования. Вы можете изменить имя издателя кода безопасности, например, если Сервер администрирования уже использует аналогичное имя издателя кода безопасности для другого Сервера администрирования. По умолчанию имя издателя кода безопасности совпадает с именем Сервера администрирования.

После изменения имени издателя кода безопасности необходимо повторно выпустить новый секретный ключ и передать его приложению для аутентификации.

Чтобы указать новое имя издателя кода безопасности:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. В открывшемся окне свойств пользователя выберите вкладку **Защита учетной записи**.

3. На вкладке **Защита учетной записи** перейдите по ссылке **Изменить**.

   Откроется раздел **Изменить издателя кода безопасности**.

4. Укажите новое имя издателя кода безопасности.

5. Нажмите на кнопку **OK**.

Для Сервера администрирования указано новое имя издателя кода безопасности.

Изменение имени издателя кода безопасности (на базе MMC)

У вас может быть несколько идентификаторов (также их называют издателями) для разных Серверов администрирования. Вы можете изменить имя издателя кода безопасности, например, Сервер администрирования уже использует аналогичное имя издателя кода безопасности для другого Сервера администрирования. По умолчанию имя издателя кода безопасности совпадает с именем Сервера администрирования.

После изменения имени издателя кода безопасности необходимо повторно выпустить новый секретный ключ и передать его приложению для аутентификации.

Чтобы указать новое имя издателя кода безопасности:

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.

2. В окне свойств Сервера администрирования в панели **Разделы** выберите раздел **Дополнительно**, а затем **Двухэтапная проверка**.

3. Укажите новое имя издателя кода безопасности в поле **Кем выдан код безопасности**.

4. Нажмите на кнопку **Применить** в разделе **Двухэтапная проверка**.

5. Нажмите на кнопку **ОК** в разделе **Двухэтапная проверка**.

Для Сервера администрирования указано новое имя издателя кода безопасности.

Настройка двухфакторной аутентификации для вашей учетной записи (Web Console)

При первом входе в Kaspersky Security Center после включения двухфакторной аутентификации откроется окно настройки двухфакторной аутентификации для вашей учетной записи.

Перед тем как настроить двухфакторную аутентификацию для своей учетной записи, убедитесь, что на мобильном устройстве установлено приложение для аутентификации.

Убедитесь, что время на устройстве с приложением для аутентификации и время на устройстве с Сервером администрирования синхронизированы с UTC с помощью внешних источников времени.

Чтобы настроить двухфакторную аутентификацию для учетной записи:

1. Сгенерируйте одноразовый код безопасности с помощью приложения для аутентификации на мобильном устройстве. Для этого выполните одно из следующих действий:

   - Введите секретный ключ в приложение для аутентификации вручную.

   - Нажмите на кнопку **Просмотреть QR-код** и отсканируйте QR-код с помощью приложения для аутентификации.

   Код безопасности отобразится на мобильном устройстве.

2. В окне настройки двухфакторной аутентификации укажите код безопасности, сгенерированный приложением для аутентификации и нажмите на кнопку **Проверить и применить**.

Двухфакторная аутентификация для вашей учетной записи настроена. У вас есть доступ к Серверу администрирования в соответствии со своими правами.

Настройка двухфакторной аутентификации для вашей учетной записи (на базе MMC)

При первом входе в Kaspersky Security Center после включения двухфакторной аутентификации откроется окно настройки двухфакторной аутентификации для вашей учетной записи.

Перед тем как настроить двухфакторную аутентификацию для своей учетной записи, убедитесь, что на мобильном устройстве установлено приложение для аутентификации. Убедитесь, что время на устройстве с приложением для аутентификации и время на устройстве с Сервером администрирования синхронизированы с UTC с помощью внешних источников времени.

Чтобы настроить двухфакторную аутентификацию для учетной записи:

1. Сгенерируйте одноразовый код безопасности с помощью приложения для аутентификации на мобильном устройстве. Для этого выполните одно из следующих действий:

   - Введите секретный ключ в приложение для аутентификации вручную.
   - Отсканируйте QR-код с помощью приложения для аутентификации.

   Код безопасности отобразится на мобильном устройстве.

2. В окне **Установить двухэтапную проверку** укажите код безопасности, сгенерированный приложением для аутентификации, и нажмите кнопку **ОК**.

Двухфакторная аутентификация для вашей учетной записи настроена. У вас есть доступ к Серверу администрирования в соответствии со своими правами.

Генерация нового секретного ключа

Вы можете сгенерировать новый секретный ключ для двухфакторной аутентификации своей учетной записи, только если вы авторизованы с помощью двухфакторной аутентификации.

Чтобы сгенерировать новый секретный ключ для учетной записи пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Нажмите на учетную запись пользователя, для которой вы хотите сгенерировать новый секретный ключ для двухфакторной аутентификации.
3. В открывшемся окне свойств пользователя выберите вкладку **Защита учетной записи**.
4. На вкладке **Защита учетной записи** перейдите по ссылке **Сгенерировать секретный ключ**.
5. В открывшемся окне двухфакторной аутентификации укажите новый ключ безопасности, сгенерированный приложением для аутентификации.
6. Нажмите на кнопку **Проверить и применить**.

Новый секретный ключ для пользователя создан.

Если вы потеряете мобильное устройство, можно установить приложение для аутентификации на другое мобильное устройство и сгенерировать новый секретный ключ для восстановления доступа к Kaspersky Security Center Web Console.

Запретить новым пользователям настраивать для себя двухэтапную проверку

Чтобы еще больше повысить безопасность доступа к Kaspersky Security Center Web Console, вы можете запретить новым пользователям настраивать для себя двухэтапную проверку.

Если этот параметр включен, пользователь с выключенной двухфакторной аутентификацией, например новый администратор домена, не сможет настроить двухфакторную аутентификацию. Следовательно, такой пользователь не может быть аутентифицирован на Сервере администрирования и не может войти в Kaspersky Security Center Web Console без одобрения другого администратора Kaspersky Security Center, у которого уже включена двухфакторная аутентификация.

Этот параметр доступен, если для всех пользователей включена двухфакторная аутентификация.

Чтобы запретить новым пользователям настраивать для себя двухэтапную проверку:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Дополнительные настройки безопасности** в окне свойств включите переключатель **Запретить новым пользователям настраивать для себя двухэтапную проверку**.

Этот параметр не влияет на учетные записи пользователей, добавленных в исключения двухэтапной проверки.

Чтобы предоставить доступ к Kaspersky Security Center Web Console пользователю с выключенной двухфакторной аутентификацией, временно выключите параметр **Запретить новым пользователям настраивать для себя двухэтапную проверку**, попросите пользователя включить двухфакторную аутентификацию, а затем включите параметр снова.

Назначение пользователя владельцем устройства Linux после установки Агента администрирования

Чтобы разрешить пользователю зарегистрироваться в качестве владельца устройства Linux:

1. В Kaspersky Security Center Web Console перейдите в раздел **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.

Если для пользователя включена двухфакторная аутентификация, вам необходимо ввести временный одноразовый пароль (TOTP) из приложения.

Пользователь зарегистрирован как владелец устройства.

Удаление пользователей или групп безопасности

Можно удалять только внутренних пользователей или группы безопасности.

Удаление пользователей или групп безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи** или **Группы**.
2. Установите флажок рядом с именем пользователя или группы безопасности, которую требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В открывшемся окне нажмите на кнопку **OK**.

Пользователь или группа безопасности удалены.

Изменение пароля учетной записи пользователя

Вам может потребоваться изменить пароль своей учетной записи или учетной записи другого пользователя, если срок действия текущего пароля истекает или если вы хотите сменить его на более надежный.

Пароль должен соответствовать следующим правилам:

- Длина пароля должна быть от 8 до 256 символов.
- Пароль должен содержать символы как минимум трех групп из списка ниже:
  - верхний регистр (A–Z);
  - нижний регистр (a–z);
  - числа (0–9);
  - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
- Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", если "." расположена перед "@".

Изменение пароля своей учетной записи

Чтобы изменить пароль вашей учетной записи:

1. В главном меню перейдите в параметры своей учетной записи и выберите **Изменение пароля**.
2. Введите текущий пароль и укажите новый пароль для подключения к Kaspersky Security Center.

   Чтобы посмотреть введенный пароль, нажмите на кнопку .
3. Если ваша учетная запись защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите учетные данные вашей учетной записи или учетной записи, у которой есть право Изменение списков управления доступом объектов в функциональной области Общие функции: Права пользователей.
4. Если двухфакторная аутентификация включена для учетной записи, которую вы использовали на предыдущем шаге, введите код безопасности, сгенерированный приложением для аутентификации на мобильном устройстве.

Изменение пароля учетной записи внутреннего пользователя

Чтобы изменить пароль учетной записи внутреннего пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Выберите учетную запись пользователя, которую требуется изменить.
3. В открывшемся окне свойств пользователя на вкладке **Общие** нажмите на кнопку **Изменение пароля**.
4. Установите новый пароль для подключения пользователя к Kaspersky Security Center.

   Чтобы посмотреть введенный пароль, нажмите на кнопку .
5. При необходимости включите параметр **Пользователю надо сменить пароль при первом входе**, чтобы принудительно изменить пароль при следующей аутентификации пользователя.
6. Если учетная запись пользователя защищена от несанкционированного изменения, вам нужно подтвердить, что у вас есть права для изменения этой учетной записи. В окне **Защита учетной записи** укажите учетные данные учетной записи, у которой есть право Изменение списков управления доступом объектов в функциональной области Общие функции: Права пользователей.
7. Если двухфакторная аутентификация включена для учетной записи, которую вы использовали на предыдущем шаге, введите код безопасности, сгенерированный приложением для аутентификации на мобильном устройстве.

Настройка параметров изменения пароля с помощью флагов сервера

Используя утилиту klscflag, вы можете настроить изменение пароля с помощью следующих команд:

- Настройка периода замены пароля (флаг `LP_SplPwdChangePeriodDays`).

  `klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <период_ротации>`

  где `<период_ротации>` – это период в днях, по истечении которого срок действия пароля пользователя истекает. Возможные значения: 0–730. Если значение параметра указано 0, смена пароля выключена.

- Настройка времени предварительного предупреждения о необходимости изменения пароля (флаг `LP_SplPwdChangeNotificationHours`).

  `klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <время_предупреждения>`

  где `<время_предупреждения>` – это период в часах, перед тем как срок действия пароля пользователя истечет. В течение этого времени отображается уведомление о необходимости изменить пароль. Возможные значения: 0–17520. Если значение параметра указано 0, время предупреждения составляет 25% от периода замены пароля.

- Указание значения по умолчанию для параметра **Пользователю надо сменить пароль при первом входе** (флаг `LP_SplPwdForceChange`).

  `klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <значение>`

  Где возможные значения флага `<значение>`:

  `1` – параметр **Пользователю надо сменить пароль при первом входе** включен.

  `0` – параметр **Пользователю надо сменить пароль при первом входе** выключен.

Чтобы просмотреть текущее значение флага, выполните следующую команду:

`klscflag.exe -fget -pv .core/.independent -s KLLIM -n <флаг> -t d`

Где `<флаг>` – это флаг `LP_SplPwdChangePeriodDays`, `LP_SplPwdChangeNotificationHours` или `LP_SplPwdForceChange`.

Создание роли пользователя

Чтобы создать роль пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Имя новой роли** укажите имя новой роли.
4. Нажмите на кнопку **ОК**, чтобы применить изменения.

5. В открывшемся окне измените параметры роли:

   - На вкладке **Общие** измените имя роли.

     Вы не можете изменять имена предопределенных ролей.

   - На вкладке **Параметры** измените область действия роли, а также политики и профили политик, связанные с ролью.

   - На вкладке **Права доступа** измените права доступа к приложениям "Лаборатории Касперского".

6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Созданная роль появится в списке ролей пользователей.

Изменение роли пользователя

Чтобы изменить роль пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.

2. Выберите роль, которую требуется изменить.

3. В открывшемся окне измените параметры роли:

   - На вкладке **Общие** измените имя роли.

     Вы не можете изменять имена предопределенных ролей.

   - На вкладке **Параметры** измените область действия роли, а также политики и профили политик, связанные с ролью.

   - На вкладке **Права доступа** измените права доступа к приложениям "Лаборатории Касперского".

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Обновленная роль появится в списке ролей пользователей.

Изменение области для роли пользователя

Область роли пользователя – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

Чтобы добавить пользователей, группы безопасности и группы администрирования в область роли пользователя, воспользуйтесь одним из следующих способов:

Способ 1:

1. В главном окне приложения перейдите в раздел U **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи** или **Группы**.

2. Установите флажки напротив имен пользователей или групп безопасности, которые требуется добавить в область роли.

3. Нажмите на кнопку **Назначить роль**.

   Будет запущен мастер назначения роли. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. На шаге **Выбор роли** выберите роль, которую требуется назначить.

5. На шаге **Определение области** выберите группу администрирования, которую требуется добавить в область роли.

6. Нажмите на кнопку **Назначить роль**, чтобы закрыть окно мастера.

Выбранные пользователи, группы безопасности и группы администрирования добавлены в область роли.

Способ 2:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.

2. Выберите роль, для которой требуется задать область.

3. В открывшемся окне свойств роли выберите вкладку **Параметры**.

4. В разделе **Область действия роли** нажмите на кнопку **Добавить**.

   Будет запущен мастер назначения роли. Для продолжения работы мастера нажмите на кнопку **Далее**.

5. На шаге **Определение области** выберите группу администрирования, которую требуется добавить в область роли.

6. На шаге **Выбор пользователей** выберите пользователей и группы безопасности, которые требуется добавить в область роли.

7. Нажмите на кнопку **Назначить роль**, чтобы закрыть окно мастера.

8. Нажмите на кнопку **Закрыть** (✕), чтобы закрыть окно свойств.

Выбранные пользователи, группы безопасности и группы администрирования добавлены в область роли.

Способ 3:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Права доступа** установите флажок рядом с именем пользователя или группы безопасности, которым вы хотите добавить область пользовательской роли, и нажмите на кнопку **Роли**.

   Вы не можете выбрать несколько пользователей или групп безопасности одновременно. Если вы выберете более одного объекта, кнопка **Роли** будет неактивна.

3. В окне **Роли** выберите пользовательскую роль, которую вы хотите назначить, примените и сохраните изменения.

   Выбранные пользователи или группы безопасности добавлены в область роли.

Удаление роли пользователя

Чтобы удалить роль пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Установите флажок напротив роли, которую требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **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 и профили политик**.
4. Нажмите на кнопку **Изменить**.

5. Чтобы связать роль с:

   - **Существующим профилем политики** – нажмите на значок (>) рядом с именем требуемой политики, а затем установите флажок рядом с профилем политики, с которым вы хотите связать роль.

   - **Новым профилем политики**:

     a. Установите флажок около политики, для которой вы хотите создать профиль политики.

     b. Нажмите на кнопку **Новый профиль политики**.

     c. Укажите имя нового профиля политики и настройте параметры профиля политики.

     d. Нажмите на кнопку **Сохранить**.

     e. Установите флажок рядом с новым профилем политики.

6. Нажмите на кнопку **Назначить роли**.

Выбранный профиль политики связывается с ролью и появляется в свойствах роли. Профиль автоматически применяется ко всем устройствам, владельцам которых назначена эта роль.

Распространение пользовательских ролей на подчиненные Серверы администрирования

По умолчанию списки пользовательских ролей главного и подчиненного Серверов администрирования являются независимыми. Вы можете настроить приложения для автоматического распространения ролей пользователей, созданных на главном Сервере администрирования, на все подчиненные Сервера администрирования. Роли пользователей также могут распространяться с подчиненного Сервера администрирования на собственные подчиненные Сервера администрирования.

Чтобы распространить роли пользователей с главного Сервера администрирования на подчиненные Серверы администрирования:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Перейдите в раздел **Иерархия Серверов администрирования**.

3. Включите параметр **Передать список ролей подчиненному Серверу администрирования** и нажмите на кнопку **Сохранить**.

Приложение копирует роли пользователей главного Сервера администрирования на подчиненные Серверы администрирования.

Если параметр **Передать список ролей подчиненному Серверу администрирования** включен и роли пользователей распространены, такие роли не доступны для изменений или удаления на подчиненном Сервере администрирования. Когда вы создаете роль или изменяете существующую роль на главном Сервере администрирования, изменения автоматически копируются на подчиненные Серверы администрирования. Когда вы удаляете роль пользователя на главном Сервере администрирования, эта роль остается на подчиненном Сервере администрирования и может быть изменена или удалена.

Роли, которые распространяются на подчиненный Сервер администрирования с главного Сервера, отображаются с помощью зеленого флажка (✓). Вы не можете изменять эти роли на подчиненном Сервере администрирования.

Если роль создается на главном Сервере администрирования, а на подчиненном Сервере администрирования есть роль с таким же именем, новая роль копируется на подчиненный Сервер администрирования, и к ее имени в скобках добавляется номер, например, ~~1, ~~2 (номер может быть случайным).

Если выключить параметр **Передать список ролей подчиненному Серверу администрирования**, все роли пользователя останутся на подчиненных Серверах администрирования, но станут независимыми от ролей на главном Сервере администрирования. Когда роли на подчиненных Серверах администрирования становятся независимыми, их можно изменять или удалять.

Смена пароля учетной записи

Вы можете изменить пароль локальной учетной записи, например, когда пользователь забыл пароль локальной учетной записи или чтобы изменить пароль по расписанию.

Изменение пароля будет применяться, даже если пользователь не вошел в учетную запись. Вы также можете изменить пароль для локальной учетной записи root.

Эту задачу можно выполнять только на устройствах под управлением Linux.

Чтобы изменить пароль локальной учетной записи на определенных устройствах:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В поле **Тип задачи** выберите **Изменить пароль учетной записи (только для Linux)**.
4. Выберите один из следующих вариантов:

   - **Назначить задачу группе администрирования**

     Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

     Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

     Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, так как групповые задачи подчиняются параметрам групп безопасности, к которым они относятся.

   - **Задать адреса устройств вручную или импортировать из списка**

     Вы можете задавать 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 *Изменить пароль учетной записи (только для Linux)* создается для указанных устройств. Если вы выбрали параметр **Назначить задачу группе администрирования**, задача является групповой.

5. На шаге **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

   Доступные параметры зависят от параметра, выбранного на предыдущем шаге.

6. На шаге **Введите имя учетной записи и новый пароль** укажите следующие параметры:

   - В поле **Имя учетной записи** укажите имя учетной записи, для которой вы хотите изменить пароль.

   - В поле **Новый пароль** укажите пароль, который будет установлен для учетной записи, указанной в предыдущем поле.

     Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

   - При необходимости установите флажок **Установить в качестве одноразового пароля (пользователь должен изменить пароль после первого входа в систему)**.

     - **Установить в качестве одноразового пароля (пользователь должен изменить пароль после первого входа в систему)**

       Если этот флажок установлен, пользователю будет предложено изменить новый пароль после первого входа в систему.

       Если этот флажок снят, пользователю не будет предлагаться изменить новый пароль после первого входа в систему.

       По умолчанию флажок снят.

7. На шаге **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

   Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи. В этом окне можно проверить параметры задачи, изменить их или при необходимости настроить расписание запуска задачи.

8. В списке задач выберите созданную задачу и нажмите на кнопку **Запустить**.

   Или дождитесь запуска задачи в соответствии с расписанием, указанным в параметрах задачи.

Когда задача изменения пароля учетной записи завершится, пароль будет изменен для указанной локальной учетной записи на выбранных устройствах.

Чтобы обеспечить корректную работу задач изменения пароля учетной записи, на пользовательском устройстве должен быть выключен SELinux.

Отзыв прав локального администратора

Вы можете отозвать права локального администратора для учетных записей. Это дает вам дополнительный уровень контроля учетных записей пользователей. Например, вы можете отозвать права локального администратора после завершения разового назначения.

При запуске этой задачи указанная локальная учетная запись проверяется на принадлежность к локальным группам администраторов, которые определены в параметрах политики Агента администрирования. Вы можете настроить список локальных групп администраторов в параметрах политики Агента администрирования. Вы также можете проверить список учетных записей привилегированных пользователей, используя **Отчет о привилегированных пользователях устройств (только для Linux)**.

Эту задачу можно выполнять только на устройствах под управлением Linux.

Чтобы отозвать права локального администратора на определенных устройствах:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В поле **Тип задачи** выберите **Отозвать права локального администратора (только для Linux)**.
4. Выберите один из следующих вариантов:

   - **Назначить задачу группе администрирования**

     Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

     Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

     Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, так как групповые задачи подчиняются параметрам групп безопасности, к которым они относятся.

   - **Задать адреса устройств вручную или импортировать из списка**

     Вы можете задавать 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.

Для указанных устройств создается задача *Отозвать права локального администратора (только для Linux)*. Если вы выбрали параметр **Назначить задачу группе администрирования**, задача является групповой.

5. На шаге **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

   Доступные параметры зависят от параметра, выбранного на предыдущем шаге.

6. На этом шаге мастера укажите следующие параметры:

   - В группе параметров **Режим работы** выберите режим работы:

     - **Отозвать права локального администратора для перечисленных учетных записей**

       Если выбран этот параметр, права локального администратора будут отозваны для указанных локальных учетных записей.

       По умолчанию выбран этот вариант.

     - **Исключить перечисленные учетные записи из списка отзыва прав локального администратора**

       Если выбран этот параметр, права локального администратора будут отозваны для всех локальных учетных записей, кроме указанных.

       По умолчанию вариант не выбран.

   - Укажите локальные учетные записи:

     - Нажмите на кнопку **Добавить**.

     - В открывшемся окне выполните одно из следующих действий:

       - В поле **Имя учетной записи** укажите имя локальной учетной записи.

       - В группе параметров **Действие учетной записи** (доступно, если выбран параметр **Отозвать права локального администратора для перечисленных учетных записей**) выберите действие.

       - **Сохранить учетную запись**

         Если выбран этот параметр, локальная учетная запись не удаляется после отзыва прав локального администратора.

         По умолчанию выбран этот вариант.

       - **Удалить учетную запись**

         Если выбран этот параметр, локальная учетная запись будет удалена независимо от того, есть ли у нее права локального администратора.

         По умолчанию вариант не выбран.

7. На шаге **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

   Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи. В этом окне можно проверить параметры задачи, изменить их или при необходимости настроить расписание запуска задачи.

8. В списке задач выберите созданную задачу и нажмите на кнопку **Запустить**.

   Или дождитесь запуска задачи в соответствии с расписанием, указанным в параметрах задачи.

После завершения задачи права локального администратора отозваны для указанных локальных учетных записей на выбранных устройствах.

Работа с ревизиями объектов

Этот раздел содержит информацию о работе с ревизиями объектов. Kaspersky Security Center позволяет отслеживать изменения объектов. Каждый раз, когда вы сохраняете изменения объекта, создается *ревизия.* Каждая ревизия имеет номер.

Объекты приложения, 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 Web Console, с помощью которого был изменен объект.
- **Действие** – выполненное действие с объектом.
- **Описание** – описание ревизии изменения параметров объекта.

  По умолчанию описание ревизии объекта не заполнено. Чтобы добавить описание ревизии, выберите нужную ревизию и нажмите на кнопку **Изменить описание**. В открывшемся окне введите текст описания ревизии.

Откат изменений объекта к предыдущей ревизии

В случае необходимости вы можете откатить изменения объекта. Например, вам может понадобиться вернуть параметры политики к состоянию на определенную дату.

Чтобы откатить изменения объекта:

1. В окне свойств объекта перейдите на вкладку **История ревизий**.
2. В списке ревизий объекта выберите ревизию, к которой нужно откатить изменения.
3. Нажмите на кнопку **Откатить**.
4. Нажмите на кнопку **OK**, чтобы подтвердить операцию.

Произойдет откат к выбранной ревизии. В списке ревизий объекта отобразится запись о выполненном действии. В описании ревизии отобразится информация о номере ревизии, к которой вы вернули объект.

Операция отката доступна только для политик и задач.

Добавление описания ревизии

Kaspersky Security Center позволяет отслеживать изменения объектов. Каждый раз, когда вы сохраняете изменения объекта, создается ревизия. Каждая ревизия имеет номер.

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.

Просмотр и сохранение ревизии политики

Kaspersky Security Center позволяет просмотреть, какие изменения были внесены в политику за определенный период, и сохранить информацию об этих изменениях в файле.

Просмотр и сохранение ревизии политики доступны, если соответствующий веб-плагин управления поддерживает эту функцию.

Чтобы просмотреть ревизию политики:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на ревизию политики, которую вы хотите просмотреть и перейдите в раздел **История ревизий**.
3. В списке ревизий политики нажмите на номер ревизии, которую вы хотите просмотреть.

   Если размер ревизии превышает 10 МБ, просмотреть ее с помощью Kaspersky Security Center Web Console невозможно. Вам будет предложено сохранить выбранную ревизию в файл JSON.

   Если размер ревизии не превышает 10 МБ, отображается отчет в формате HTML с параметрами выбранной ревизии политики. Так как отчет отображается во всплывающем окне, убедитесь, что в вашем браузере разрешены всплывающие окна.

Чтобы сохранить ревизию политики в файл JSON,

В списке ревизий политики выберите ревизию, которую вы хотите сохранить и нажмите на кнопку **Сохранить в файл**.

Ревизия сохранена в файле JSON.

Удаление объектов

В этом разделе приведена информация об удалении объектов.

Вы можете удалять следующие объекты:

- политики;
- задачи;
- инсталляционные пакеты;
- виртуальные Серверы администрирования;
- пользователей;
- группы безопасности;
- группы администрирования.

Чтобы удалить объект:

1. Откройте нужный раздел в Kaspersky Security Center Web Console и выберите объект.
2. В панели инструментов нажмите на кнопку **Удалить**.
3. В появившемся окне нажмите на кнопку **OK**, чтобы подтвердить свой выбор.

   Выбранный объект будет удален.

Когда вы удаляете объект, информация об этом записывается в базу данных. Срок хранения информации об удаленных объектах такой же, как и срок хранения ревизий объектов (рекомендуемый срок 90 дней). Можно изменить время хранения только при наличии права на **Изменение** для области **Удаленные объекты**.

Об удалении клиентских устройств

При удалении управляемого устройства из группы администрирования приложение перемещает устройство в группу Нераспределенные устройства. После удаления устройства установленные приложения "Лаборатории Касперского" – Агент администрирования и приложение безопасности, например Kaspersky Endpoint Security, – остаются на устройстве.

Kaspersky Security Center обрабатывает устройства из группы Нераспределенные устройства по следующим правилам:

- Если вы настроили правила перемещения устройств и устройство соответствует критериям правила перемещения, устройство автоматически перемещается в группу администрирования в соответствии с правилом.
- Устройство сохраняется в группе Нераспределенные устройства и автоматически удаляется из группы в соответствии с правилами хранения устройств.

  Правила хранения устройств не влияют на устройства, на которых один или несколько дисков зашифрованы с помощью полнодискового шифрования. Такие устройства не удаляются автоматически – вы можете удалить их только вручную. Если вам нужно удалить устройство с зашифрованным жестким диском, сначала расшифруйте диск, а затем удалите устройство.

  > При удалении устройства с зашифрованным жестким диском данные, необходимые для расшифровки диска, также удаляются. Если вы установите флажок **Я понимаю риск и хочу удалить выбранные устройства** в окне подтверждения, которое открывается при удалении таких устройств (из группы **Нераспределенные устройства** или из группы **Управляемые устройства**), это означает, что вы знаете о последующем удалении данных.

  В этом случае для расшифровки диска требуется выполнение следующих условий:

  - Устройство повторно подключается к Серверу администрирования для восстановления данных, необходимых для расшифровки диска.
  - Пользователь устройства помнит пароль для расшифровки.
  - Приложение безопасности, которое использовалось для шифрования диска, например Kaspersky Endpoint Security для Windows, установлено на устройстве.

Если диск был зашифрован с помощью технологии Kaspersky Disk Encryption, вы также можете попробовать восстановить данные с помощью утилиты FDERT Restore.

В VDI, если у вас есть устройство с зашифрованными жесткими дисками, информация на зашифрованном диске удаляется после удаления устройства.

При удалении устройства из группы Нераспределенные устройства вручную приложение удаляет устройство из списка. После удаления устройства установленные приложения "Лаборатории Касперского" (если они есть) остаются на устройстве. Затем, если устройство по-прежнему видно Серверу администрирования и вы настроили регулярный опрос сети, Kaspersky Security Center 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.

Kaspersky Security Network (KSN)

В этом разделе описано использование инфраструктуры онлайн-служб Kaspersky Security Network (KSN). Приведена информация о KSN, а также инструкции по включению KSN, настройке доступа к KSN, по просмотру статистики использования прокси-сервера KSN.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

О KSN

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. KSN позволяет получать из репутационных баз "Лаборатории Касперского" информацию о приложениях, установленных на управляемых устройствах.

Kaspersky Security Center поддерживает следующие инфраструктурные решения:

- *KSN* – решение, позволяющее обмениваться информацией с Kaspersky Security Network. Участвуя в программе KSN, вы соглашаетесь в автоматическом режиме предоставлять в "Лабораторию Касперского" информацию о работе приложений "Лаборатории Касперского", установленных на клиентских устройствах, находящихся под управлением Kaspersky Security Center. Передача информации выполняется в соответствии с настроенными параметрами доступа к KSN. Эксперты "Лаборатории Касперского" дополнительно анализируют полученную информацию и включают ее в репутационные и статистические базы данных Kaspersky Security Network. Kaspersky Security Center использует это решение по умолчанию.

- *Kaspersky Private Security Network (KPSN)* – это решение, которое предоставляет пользователям устройств с установленными приложениями "Лаборатории Касперского" доступ к репутационным базам Kaspersky Security Network и другим статистическим данным без отправки данных со своих устройств в Глобальный KSN. KPSN предназначен для организаций, которые не могут участвовать в Kaspersky Security Network по одной из следующих причин:

  - Устройства пользователей не подключены к интернету.

  - Передача любых данных за пределы страны или корпоративной сети (LAN) запрещена законом или корпоративными политиками безопасности.

  Вы можете настроить параметры доступа Kaspersky Private Security Network в разделе **Параметры прокси-сервера KSN** окна свойств Сервера администрирования.

Приложение предлагает присоединиться к KSN во время работы мастера первоначальной настройки. Вы можете начать использование KSN или отказаться от использования KSN в любой момент работы с приложением.

Вы используете KSN в соответствии с Положением о KSN, которое вы читаете и принимаете при включении KSN. Если Положение о KSN обновлено, оно отображается при обновлении Сервера администрирования с предыдущей версии. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с предыдущей версией Положения о KSN, которую вы приняли ранее.

Когда KSN включен, Kaspersky Security Center 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, получать информацию от KSN и передавать в KSN информацию, даже если они не имеют прямого доступа в интернет.

- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентским устройством запрошенной информации.

Вы можете настроить параметры прокси-сервера KSN в разделе **Параметры прокси-сервера KSN** окна свойств Сервера администрирования.

Настройка доступа к KSN

Можно задать доступ к Kaspersky Security Network (KSN) с Сервера администрирования и с точки распространения.

Чтобы настроить доступ Сервера администрирования к KSN:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.

3. Переведите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования Включено**.

   Если этот параметр включен, прокси-сервер KSN отправляет данные в KSN для повышения эффективности работы компонентов Kaspersky Security Center и приложений "Лаборатории Касперского". Передача данных от клиентских устройств в KSN регулируется политикой Kaspersky Endpoint Security, действующей на клиентских устройствах. Если переключатель выключен, передача данных в KSN от Сервера администрирования и от клиентских устройств через Kaspersky Security Center не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky Security Center). Действующая на клиентских устройствах политика Kaspersky Endpoint Security определяет, какие данные эти устройства напрямую (не через Kaspersky Security Center) передают в KSN.

4. Переведите переключатель в положение **Использовать Kaspersky Security Network Включено**.

   Если параметр включен, клиентские устройства будут передавать результаты установки патчей в "Лабораторию Касперского". При включении этого параметра убедитесь, что вы прочитали и принимаете условия Положения о KSN.

   Если вы используете KPSN, переведите переключатель в положение **Использовать Kaspersky Private Security Network Включено** и нажмите на кнопку **Файл с параметрами прокси-сервера KSN**, чтобы загрузить параметры KPSN (файлы с расширениями pkcs7 и pem). После загрузки параметров в интерфейсе отображаются наименование провайдера, контакты провайдера и дата создания файла с параметрами KPSN.

   > При включении KPSN обратите внимание на точки распространения настроенные на отправление KSN запросов напрямую облачной-службе KSN. Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к облачной-службе KSN. Чтобы перенастроить точки распространения для отправки запросов KSN в KPSN, включите параметр **Пересылать KSN запрос Серверу администрирования** для каждой точки распространения. Вы можете включить этот параметр в свойствах точки распространения или политики Агента администрирования.

   При переводе переключателя в положение **Использовать Kaspersky Private Security Network Включено** появится сообщение с подробной информацией о KPSN.

   KPSN поддерживают следующие приложения "Лаборатории Касперского":

   - Kaspersky Security Center
   - Kaspersky Endpoint Security для Windows

- Kaspersky Endpoint Security для Linux
- Kaspersky Security для виртуальных сред 3.0 Защита без агента Service Pack 2
- Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент

Если вы включите KPSN в Kaspersky Security Center, эти приложения получат об этом информацию о поддержке KPSN. В окне свойств приложения в подразделе **Kaspersky Security Network** раздела **Продвинутая защита** отображается поставщик KSN: KSN или KPSN.

Если для работы с KPSN вы используете версии приложений ниже Kaspersky Security для виртуальных сред 3.0 Защита без агента Service Pack 2 или ниже Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент, рекомендуется использовать подчиненные Серверы администрирования, для которых не настроено использование KPSN.

Kaspersky Security Center не отправляет статистику Kaspersky Security Network, если настроен KPSN в окне свойств Сервера администрирования в разделе **Параметры прокси-сервера KSN**.

5. Установите флажок **Игнорировать параметры прокси-сервера для подключения к KPSN**, если в свойствах Сервера администрирования настроены параметры прокси-сервера, но архитектура сети требует работы с KPSN напрямую. В противном случае запрос от управляемого приложения не будет передан в KPSN.

6. Настройте параметры подключения Сервера администрирования к службе прокси-сервера KSN:

   - В блоке **Параметры подключения**, в поле ввода **TCP-порт**, укажите номер TCP-порта, через который будет выполняться подключение к прокси-серверу KSN. По умолчанию подключение к прокси-серверу KSN выполняется через порт 13111.
   - Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, выберите параметр **Использовать UDP-порт** и в поле **UDP-порт** укажите номер порта. По умолчанию параметр выключен, используется порт TCP. Если параметр включен, по умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.
   - Чтобы Сервер администрирования подключался к прокси-серверу KSN через HTTPS-порт, выберите параметр **Использовать HTTPS** и в поле **Через HTTPS-порт** укажите номер порта. По умолчанию параметр выключен, используется порт TCP. Если параметр включен, по умолчанию подключение к прокси-серверу KSN выполняется через HTTPS-порт 17111.

7. Переведите переключатель в положение **Подключать подчиненные Серверы администрирования к KSN через главный Сервер Включено**.

   Если этот параметр включен, подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера KSN. Если этот параметр выключен, подчиненные Серверы администрирования подключаются к KSN самостоятельно. В этом случае управляемые устройства используют подчиненные Серверы администрирования как прокси-серверы KSN.

   Подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера, если в свойствах подчиненных Серверов администрирования в разделе **Параметры прокси-сервера KSN** также переключатель переведен в положение **Включить прокси-сервер KSN на Сервере администрирования Включено**.

8. Нажмите на кнопку **Сохранить**.

В результате параметры доступа к KSN будут сохранены.

Можно также настроить доступ к KSN со стороны точки распространения, например, если необходимо снизить нагрузку на Сервер администрирования. Точка распространения, выполняющая роль прокси-сервера KSN, отправляет KSN запросы от управляемых устройств напрямую в "Лабораторию Касперского", минуя Сервер администрирования.

Чтобы настроить доступ точки распространения к Kaspersky Security Network (KSN):

1. Убедитесь, что точка распространения была назначена вручную.
2. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
3. На вкладке **Общие** выберите раздел **Точки распространения**.
4. Нажмите на имя точки распространения, чтобы открыть окно ее свойств.
5. В окне свойств точки распространения в разделе **Прокси-сервер KSN**, включите параметр **Включить прокси-сервер KSN на стороне точки распространения** и параметр **Доступ к облачной службе KSN/KPSN непосредственно через интернет**.
6. Нажмите на кнопку **OK**.

Точка распространения будет исполнять роль прокси-сервера KSN.

Включение и выключение использования KSN

Чтобы включить использование KSN:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На вкладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.
3. Переведите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования Включено**.

Прокси-сервер KSN включен и отправляет данные в KSN для повышения эффективности работы компонентов Kaspersky Security Center и производительности приложений "Лаборатории Касперского".

1. В зависимости от используемого решения инфраструктуры KSN, включите соответствующие переключатели.

   - Если вы используете Глобальный KSN, переведите переключатель в положение **Использовать Kaspersky Security Network Включено**.

     Теперь доступна отправка данных в KSN. При включении этого параметра, вам нужно прочитать и принять условия Положения о KSN.

- Если вы используете KPSN, переведите переключатель в положение **Использовать Kaspersky Private Security Network Включено** и нажмите на кнопку **Файл с параметрами прокси-сервера KSN**, чтобы загрузить параметры KPSN (файлы с расширениями pkcs7 и pem). После загрузки параметров в интерфейсе отображаются наименование провайдера, контакты провайдера и дата создания файла с параметрами KPSN.

  При переводе переключателя в положение **Использовать Kaspersky Private Security Network Включено** появится сообщение с подробной информацией о KPSN.

2. Нажмите на кнопку **Сохранить**.

Чтобы выключить использование KSN:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.

3. Переключите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования Выключено**, чтобы выключить службу прокси-сервера KSN.

4. Нажмите на кнопку **Сохранить**.

Просмотр принятого Положения о KSN

При включении Kaspersky Security Network (KSN) вам нужно прочитать и принять Положение о KSN. Вы можете просмотреть принятое Положение о KSN в любое время.

Чтобы просмотреть принятое Положение о KSN:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.

3. Перейдите по ссылке **Просмотреть Положение о Kaspersky Security Network**.

В открывшемся окне вы можете просмотреть текст принятого Положения о KSN.

Принятие обновленного Положения о KSN

Вы используете KSN в соответствии с Положением о KSN, которое вы читаете и принимаете при включении KSN. Если Положение о KSN обновлено, оно отображается при обновлении Сервера администрирования с предыдущей версии. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с версией Положения о KSN, которую вы приняли ранее.

После обновления Сервера администрирования с предыдущей версии обновленное Положение о KSN отображается автоматически. Если вы отклоните обновленное Положение о KSN, вы все равно сможете просмотреть и принять его позже.

Чтобы просмотреть и принять или отклонить обновленное Положение о KSN:

1. Нажмите на значок **Просмотреть уведомления о событиях** в правом верхнем углу главного окна приложения.

   Откроется окно **Уведомления**.

2. Перейдите по ссылке **Просмотреть обновленное Положение о KSN**.

   Откроется окно **Обновление Положения о Kaspersky Security Network**.

3. Прочтите Положение о KSN, а затем примите решение, нажав одну из следующих кнопок:

   - **Я принимаю условия обновленного Положения о KSN**
   - **Использовать KSN со старым Положением о KSN**

В зависимости от вашего выбора KSN продолжит работу в соответствии с условиями текущего или обновленного Положения о KSN. Вы можете в любой момент просмотреть текст принятого Положения о KSN в свойствах Сервера администрирования.

Проверка, работает ли точка распространения как прокси-сервер KSN

На управляемом устройстве, которое выполняет роль точки распространения, вы можете включить прокси-сервер 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.

Сценарий: обновление Kaspersky Security Center и управляемых приложений безопасности

В этом разделе описан основной сценарий обновления приложения Kaspersky Security Center и управляемых приложений безопасности.

Обновление Kaspersky Security Center и управляемых приложений безопасности состоит из следующих этапов:

1. **Проверка требований к оборудованию и программному обеспечению**

   Убедитесь, что ваше оборудование соответствует требованиям, и установите необходимые обновления.

2. **Планирование ресурсов**

   Оцените, сколько дискового пространства занимает ваша база данных. Убедитесь, что на жестком диске имеется достаточно свободного места для хранения резервной копии данных Сервера администрирования.

3. **Получение файла установки Kaspersky Security Center**

   Получите исполняемый файл для текущей версии Kaspersky Security Center и сохраните его на устройство, выполняющее роль Сервера администрирования. Ознакомьтесь с информацией о выпуске для версии Kaspersky Security Center, которую вы используете.

4. **Создание резервной копии предыдущей версии**

   С помощью утилиты резервного копирования и восстановления данных создайте резервную копию данных Сервера администрирования. Вы также можете создать задачу резервного копирования.

   Рекомендуется экспортировать список установленных плагинов.

5. **Запуск установщика**

   Запустите исполняемый файл для последней версии Kaspersky Security Center. После запуска файла укажите, что была создана резервная копия, а также путь к ней. Будет выполнено восстановление данных из резервной копии.

6. **Обновление управляемых приложений**

   Можно обновить приложение, если доступна новая версия. Ознакомьтесь со списком поддерживаемых приложений "Лаборатории Касперского" и убедитесь, что ваша версия Kaspersky Security Center совместима с этим приложением. Затем обновите приложение, как описано в информации о выпуске.

Результаты

После завершения сценария обновления убедитесь, что новая версия Сервера администрирования успешно установлена в Консоли управления (MMC). В меню выберите **Справка → О Kaspersky Security Center**. Отобразится номер версии приложения.

Убедитесь, что вы используете последнюю версию Сервера администрирования в Kaspersky Security Center Web Console, в верхней части экрана нажмите значок параметров () рядом с именем Сервера администрирования. В открывшемся окне свойств Сервер администрирования на вкладке **Общие** выберите раздел **Общие**. Отобразится номер версии приложения.

Если вам нужно восстановить данные Сервера администрирования, выполните действия, описанные в следующем разделе: Резервное копирование и восстановление данных в интерактивном режиме.

Если вы обновили управляемое приложение безопасности, убедитесь, что она установлена правильно на управляемых устройствах. Дополнительную информацию см. в документации к этому приложению.

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 и приложений безопасности.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"

В этом разделе представлен сценарий регулярного обновления баз данных, модулей приложений и приложений "Лаборатории Касперского". После того, как вы завершили сценарий Настройка защиты в сети организации, вам нужно поддерживать надежность системы защиты, чтобы обеспечить защиту Серверов администрирования и управляемых устройств от различных угроз, включая вирусы, сетевые атаки и фишинговые атаки.

Защита сети поддерживается обновленной с помощью регулярных обновлений следующего:

- баз и модулей приложений "Лаборатории Касперского";
- установленных приложений "Лаборатории Касперского", включая компоненты Kaspersky Security Center и приложений безопасности.

Когда вы завершите этот сценарий, вы можете быть уверены, что:

- Ваша сеть защищена самым последним программным обеспечением "Лаборатории Касперского", включая компоненты Kaspersky Security Center и приложения безопасности.
- Антивирусные базы и другие базы данных "Лаборатории Касперского", критически важные для безопасности сети, всегда актуальны.

Предварительные требования

Управляемые устройства должны иметь соединение с Сервером администрирования. Если у устройств нет соединения, рассмотрите возможность обновления баз, модулей приложений и приложений "Лаборатории Касперского" вручную или напрямую с серверов обновлений "Лаборатории Касперского".

Сервер администрирования должен иметь подключение к интернету.

Прежде чем приступать, убедитесь, что вы выполнили следующее:

1. Развернуты приложения безопасности "Лаборатории Касперского" на управляемых устройствах в соответствии со сценарием развертывания приложений "Лаборатории Касперского" с помощью Kaspersky Security Center Web Console.

2. Созданы и настроены все необходимые политики, профили политик и задачи в соответствии со сценарием настройки защиты сети.

3. Назначено соответствующее количество точек распространения в соответствии с количеством управляемых устройств и топологией сети.

Обновление баз и приложений "Лаборатории Касперского" состоит из следующих этапов:

1. **Выбор схемы обновления**

   Существует несколько схем, которые вы можете использовать для установки обновлений компонентов Kaspersky Security Center и приложений безопасности. Выберите схему или несколько схем, которые лучше всего соответствуют требованиям вашей сети.

2. **Создание задачи для загрузки обновлений в хранилище Сервера администрирования**

   Эта задача автоматически создается в мастере первоначальной настройки Kaspersky Security Center. Если вы не запускали мастер первоначальной настройки, создайте задачу сейчас.

   Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования, а также обновления баз и модулей приложений для Kaspersky Security Center. После загрузки обновлений их можно распространять на управляемые устройства.

   Если в вашей сети назначены точки распространения, обновления автоматически загружаются из хранилища Сервера администрирования в хранилища точек распространения. В этом случае управляемые устройства, входящие в область действия точки распространения, загружают обновления из хранилищ точек распространения, вместо хранилища Сервера администрирования.

   Инструкции:

   - Консоль администрирования: Создание задачи для загрузки обновлений в хранилище Сервера администрирования.

   - Kaspersky Security Center Web Console: Создание задачи для загрузки обновлений в хранилище Сервера администрирования.

3. **Создание задачи загрузки обновлений в хранилища точек распространения (если требуется)**

По умолчанию обновления загружаются в хранилища точек распространения из хранилища Сервера администрирования. Вы можете настроить Kaspersky Security Center так, чтобы точки распространения загружали обновления непосредственно с серверов обновлений "Лаборатории Касперского". Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.

Когда вашей сети назначены точки распространения и создана задача *Загрузка обновлений в хранилища точек распространения*, точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

Инструкции:

- Консоль администрирования: Создание задачи загрузки обновлений в хранилища точек распространения.
- Kaspersky Security Center Web Console: Создание задачи загрузки обновлений в хранилища точек распространения.

4. **Настройка точек распространения**

Если в вашей сети назначены точки распространения, убедитесь, что параметр **Распространять обновления** включен в свойствах всех требуемых точек распространения. Если этот параметр выключен для точки распространения, устройства, включенные в область действия точки распространения, загружают обновления из хранилища Сервера администрирования.

Если вы хотите, чтобы управляемые устройства получали обновления только от точек распространения, включите параметр **Распространять файлы только через точки распространения** в политике Агента администрирования.

5. **Оптимизация процесса обновления с использованием офлайн-модели получения обновлений или загрузки файлов различий (если требуется)**

Вы можете оптимизировать процесс обновления, используя офлайн-модель загрузки обновлений (включена по умолчанию), или используя файлы различий. Для каждого сегмента сети вам нужно выбрать, какую из этих двух функций включить, так как они не могут работать одновременно.

Когда офлайн-модель получения обновлений включена, Агент администрирования загружает необходимые обновления на управляемое устройство после загрузки обновлений в хранилище Сервера администрирования, прежде чем приложение безопасности запросит обновления. Это повышает надежность процесса обновления. Чтобы использовать эту функцию, включите параметр **Загружать обновления и антивирусные базы с Сервера администрирования заранее (рекомендуется)** в свойствах задачи Политика Агента администрирования.

Если вы не используете офлайн-модель загрузки обновлений, вы можете оптимизировать трафик между Сервером администрирования и управляемыми устройствами, используя файлы различий. Когда эта функция включена, Сервер администрирования или точка распространения загружает файлы различий вместо целых файлов баз данных или модулей приложений "Лаборатории Касперского". Файл различий описывает различия между двумя версиями файлов базы или модулями приложения. Поэтому файлы различий занимают меньше места, чем целые файлы. В результате уменьшается трафик между Сервером администрирования или точками распространения и управляемыми устройствами. Чтобы использовать эту функцию, включите параметр **Загрузить файлы различий** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования* и/или *Загрузка обновлений в хранилища точек распространения*.

Инструкции:

- Использование файлов различий для обновления баз и модулей приложений "Лаборатории Касперского".
- Консоль администрирования: Включение и выключение офлайн-модели получения обновлений.
- Kaspersky Security Center Web Console: Консоль администрирования: Включение и выключение офлайн-модели получения обновлений.

6. **Проверка полученных обновлений (если требуется)**

   Перед установкой загруженных обновлений вы можете проверить обновления с помощью задачи *Проверка обновлений*. Эта задача последовательно запускает задачи обновления устройства и задачи поиска вредоносного ПО, настроенные с помощью параметров для указанного набора тестовых устройств. После получения результатов задачи Сервер администрирования запустит или заблокирует распространение обновлений на оставшиеся устройства.

   Задача *Проверка обновлений* может быть выполнена как часть задачи *Загрузка обновлений в хранилище Сервера администрирования*. В свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования* включите параметр **Выполнять проверку обновлений перед распространением** в Консоли администрирования или параметр **Выполнить проверку обновлений** в Kaspersky Security Center Web Console.

   Инструкции:

   - Консоль администрирования: Проверка полученных обновлений.
   - Kaspersky Security Center Web Console: Проверка полученных обновлений.

7. **Одобрение и отклонение обновлений программного обеспечения**

   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 требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства. Неопределенные обновления могут быть установлены только на Агенте администрирования и других компонентах Kaspersky Security Center в соответствии с параметрами политики Агента администрирования. Обновления, которым вы установили статус *Отклонено*, не устанавливаются на управляемые устройства. Если ранее отклоненное обновление для приложения безопасности было установлено, Kaspersky Security Center попытается удалить обновления со всех устройств.

   Одобрение и отклонение обновлений доступно только для Агента администрирования и управляемых приложений "Лаборатории Касперского", установленных на клиентских устройствах под управлением Windows и Linux. Бесшовное обновление Сервера администрирования, Kaspersky Security Center Web Console и веб-плагинов управления не поддерживается.

   Инструкции:

   - Консоль администрирования: Одобрение и отклонение обновлений программного обеспечения.
   - Kaspersky Security Center Web Console: Одобрение и отклонение обновлений программного обеспечения.

8. **Настройка автоматической установки обновлений и патчей для компонентов Kaspersky Security Center**

Загруженные обновления и патчи для Агента администрирования и других компонентов Kaspersky Security Center 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*.

Инструкции:

- Консоль администрирования: Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center.
- Kaspersky Security Center Web Console: Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center.

9. **Установка обновлений для Сервера администрирования**

   Обновления программного обеспечения для Сервера администрирования не зависят от статусов обновлений. Они не устанавливаются автоматически и должны быть предварительно одобрены администратором на вкладке **Мониторинг** в Консоли администрирования (**Сервер администрирования** `<имя Сервера>` → **Мониторинг**) или в разделе **Уведомления** в Kaspersky Security Center Web Console (**Мониторинг и отчеты** → **Уведомления**). После этого администратор должен явно запустить установку обновлений.

10. **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 выбрать параметр **При загрузке обновлений в хранилище** при настройке расписания задач для своевременного обновления.

    Если в вашей сети есть устройства, поддерживающие только IPv6, и вы хотите регулярно обновлять приложения безопасности, установленные на этих устройствах, убедитесь, что на управляемых устройствах установлены Сервер администрирования (версии 13.2 или выше) и Агент администрирования (версии 13.2 или выше).

    По умолчанию обновления для Kaspersky Endpoint Security для Windows и для Kaspersky Endpoint Security для Linux устанавливаются только после изменения статуса обновления на *Одобрено*. 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.

    Инструкции:

    - Консоль администрирования: Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства.
    - Kaspersky Security Center Web Console: Консоль администрирования: Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства.

Результаты

По завершении сценария Kaspersky Security Center настроен для обновления баз "Лаборатории Касперского" и установленных приложений "Лаборатории Касперского" после загрузки обновлений в хранилище Сервера администрирования или в хранилища точек распространения. Теперь вы можете приступить к мониторингу состояния сети.

Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"

Чтобы убедиться, что защита ваших Серверов администрирования и управляемых устройств актуальна, вам нужно своевременно предоставлять обновления следующего:

- Баз и модулей приложений "Лаборатории Касперского".

  Kaspersky Security Center проверяет доступность серверов "Лаборатории Касперского" перед загрузкой баз и 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 и приложений безопасности.

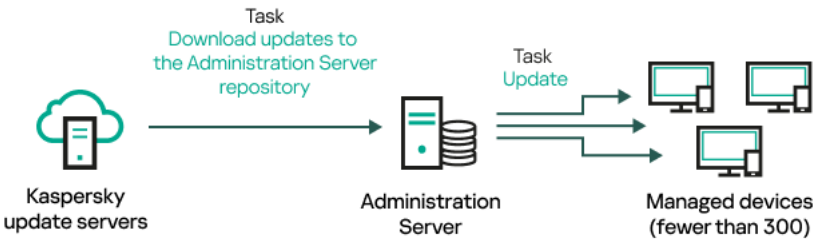
  Kaspersky Security Center позволяет автоматически обновлять Агент администрирования и приложения "Лаборатории Касперского", установленные на клиентских устройствах под управлением Windows и Linux. Бесшовное обновление Сервера администрирования, Kaspersky Security Center Web Console и веб-плагинов управления не поддерживается. Для обновления этих компонентов вам необходимо скачать их последние версии с сайта "Лаборатории Касперского" и установить их вручную.

В зависимости от конфигурации вашей сети вы можете использовать следующие схемы загрузки и распространения необходимых обновлений на управляемые устройства:

- С помощью одной задачи: *Загрузка обновлений в хранилище Сервера администрирования*
- С помощью двух задач:
  - Задача *Загрузка обновлений в хранилище Сервера администрирования*.
  - Задача *Загрузка обновлений в хранилища точек распространения*.
- Вручную через локальную папку, общую папку или FTP-сервер
- Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security на управляемых устройствах
- Через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

Использование задачи Загрузка обновлений в хранилище Сервера администрирования

В этой схеме Kaspersky Security Center загружает обновления с помощью задачи *Загрузка обновлений в хранилище Сервера администрирования*. В небольших сетях, которые содержат менее 300 управляемых устройств в одном сегменте сети или менее десяти управляемых устройств в каждом сегменте, обновления распространяются на управляемые устройства непосредственно из хранилища Сервера администрирования (см. рисунок ниже).

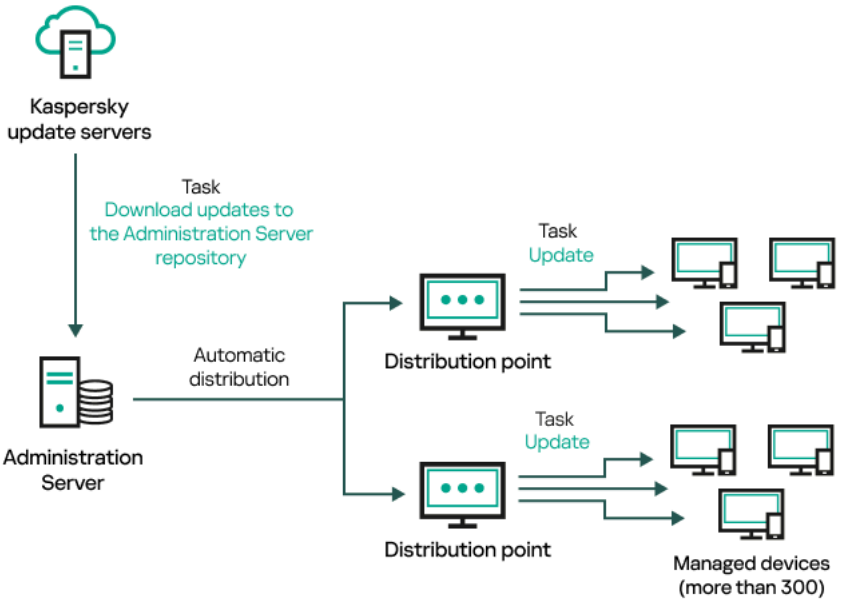


Обновление с использованием задачи Загрузка обновлений в хранилище Сервера администрирования и без точек распространения

По умолчанию Сервер администрирования взаимодействует с серверами обновлений "Лаборатории Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.

Если ваша сеть содержит более 300 управляемых устройств в одном сегменте сети или ваша сеть содержит несколько сегментов, в которых больше девяти управляемых устройств, мы рекомендуем использовать точки распространения для распространения обновлений на управляемые устройства (см. рисунок ниже). Точки распространения уменьшают загрузку Сервера администрирования и оптимизируют трафик между Сервером администрирования и управляемыми устройствами. Вы можете рассчитать количество точек распространения и их конфигурацию, необходимые для вашей сети.

В этой схеме обновления автоматически загружаются из хранилища Сервера администрирования в хранилища точек распространения. Управляемые устройства, входящие в область действия точки распространения, загружают обновления из хранилищ точек распространения, вместо хранилища Сервера администрирования.



Обновление с использованием задачи Загрузка обновлений в хранилище Сервера администрирования с точками распространения

После завершения задачи *Загрузка обновлений в хранилище Сервера администрирования* следующие обновления загружаются в хранилище Сервера администрирования:

- Базы и модули приложений "Лаборатории Касперского" для Kaspersky Security Center.

  Эти обновления устанавливаются автоматически.

- 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 Сервера администрирования.

  Эти обновления не устанавливаются автоматически. Администратор должен явно одобрить обновления и запустить установку обновлений.

  > Для установки патчей на Сервере администрирования требуются права локального администратора.

- Обновления для компонентов Kaspersky Security Center.

  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. (Вы можете одобрить обновления с помощью Консоли администрирования или Kaspersky Security Center Web Console). Обновления устанавливаются с помощью задачи *Обновление* и могут быть настроены в свойствах этой задачи.

> Задача *Загрузка обновлений в хранилище Сервера администрирования* недоступна на виртуальных Серверах администрирования. В хранилище виртуального Сервера отображаются обновления, загруженные на главный Сервер администрирования.

Вы можете настроить проверку полученных обновлений на работоспособность и на наличие ошибок на наборе тестовых устройств. Если проверка прошла успешно, обновления распространяются на другие управляемые устройства.

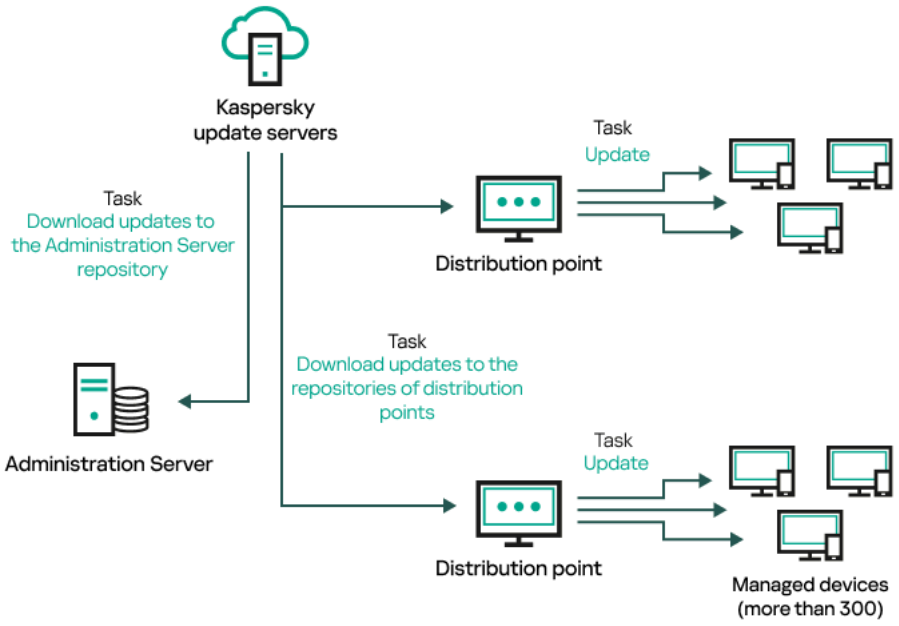
Каждое управляемое приложение "Лаборатории Касперского" запрашивает требуемые обновления с Сервера администрирования. Сервер администрирования объединяет эти запросы и загружает только те обновления, которые запрашиваются приложениями. Это обеспечивает то, что загружаются только нужные обновления и только один раз. При выполнении задачи *Загрузка обновлений в хранилище Сервера администрирования*, для обеспечения загрузки необходимых версий баз и модулей приложений "Лаборатории Касперского", на серверы обновлений "Лаборатории Касперского" автоматически, Сервер администрирования отправляет следующую информацию:

- идентификатор и версия приложения;
- идентификатор установки приложения;
- идентификатор активного ключа;
- идентификатор запуска задачи *Загрузка обновлений в хранилище Сервера администрирования*.

Передаваемая информация не содержит персональных данных и других конфиденциальных данных. АО "Лаборатория Касперского" защищает полученную информацию в соответствии с установленными законом требованиями.

Использование двух задач: Загрузка обновлений в хранилище Сервера администрирования и Загрузка обновлений в хранилища точек распространения

Вы можете загружать обновления в хранилища точек распространения непосредственно с серверов обновлений "Лаборатории Касперского" вместо хранилища Сервера администрирования, а затем распространять обновления на управляемые устройства (см. рисунок ниже). Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.



Обновление с использованием задачи Загрузка обновлений в хранилище Сервера администрирования и задачи Загрузка обновлений в хранилища точек распространения

По умолчанию Сервер администрирования и точки распространения взаимодействуют с серверами обновлений "Лаборатории Касперского" и загружают обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования и/или точки распространения на использование протокола HTTP вместо HTTPS.

Для реализации этой схемы создайте задачу *Загрузка обновлений в хранилища точек распространения* в дополнение к задаче *Загрузка обновлений в хранилище Сервера администрирования*. После этого точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

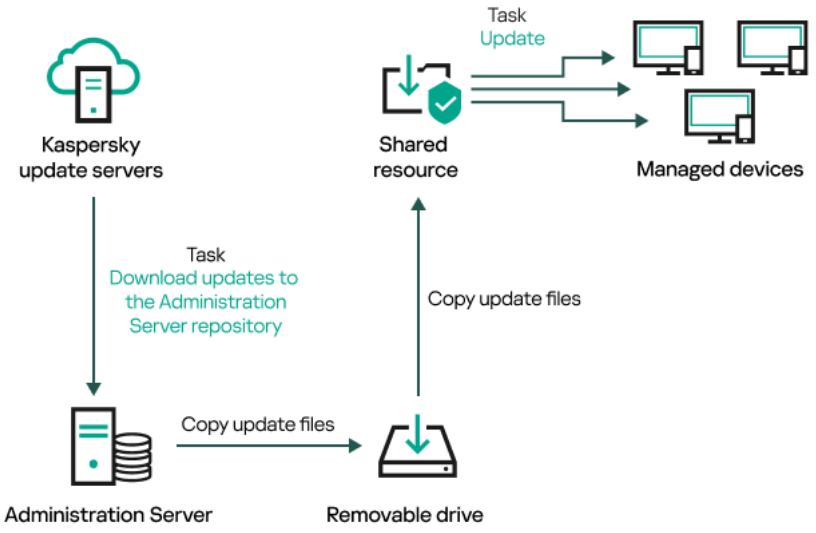
Точки распространения под управлением macOS не могут загружать обновления с серверов обновлений "Лаборатории Касперского".

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.

Для этой схемы также требуется задача *Загрузка обновлений в хранилище Сервера администрирования*, так как эта задача используется для загрузки баз и модулей приложений "Лаборатории Касперского" для Kaspersky Security Center.

Вручную через локальную папку, общую папку или FTP-сервер

Если клиентские устройства не подключены к Серверу администрирования, вы можете использовать локальную папку или общий ресурс в качестве источника обновления баз, модулей приложений и приложений "Лаборатории Касперского". В этой схеме вам нужно скопировать необходимые обновления из хранилища Сервера администрирования на съемный диск, а затем скопировать обновления в локальную папку или общий ресурс, указанный в качестве источника обновлений в параметрах Kaspersky Endpoint Security (см. рисунок ниже).



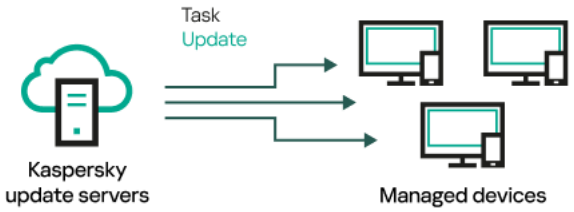
Обновление через локальную папку, общую папку или FTP-сервер

Подробнее об источниках обновлений в Kaspersky Endpoint Security см. в следующих справках:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux

Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security на управляемых устройствах

На управляемых устройствах вы можете настроить Kaspersky Endpoint Security на получение обновлений напрямую с серверов обновлений "Лаборатории Касперского" (см. рисунок ниже).



Обновление приложений безопасности непосредственно с серверов обновлений "Лаборатории Касперского"

В этой схеме приложения безопасности не используют хранилища, предоставленные Kaspersky Security Center. Чтобы получать обновления непосредственно с серверов обновлений "Лаборатории Касперского", укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений в интерфейсе программы безопасности. Дополнительные сведения об этих параметрах см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux

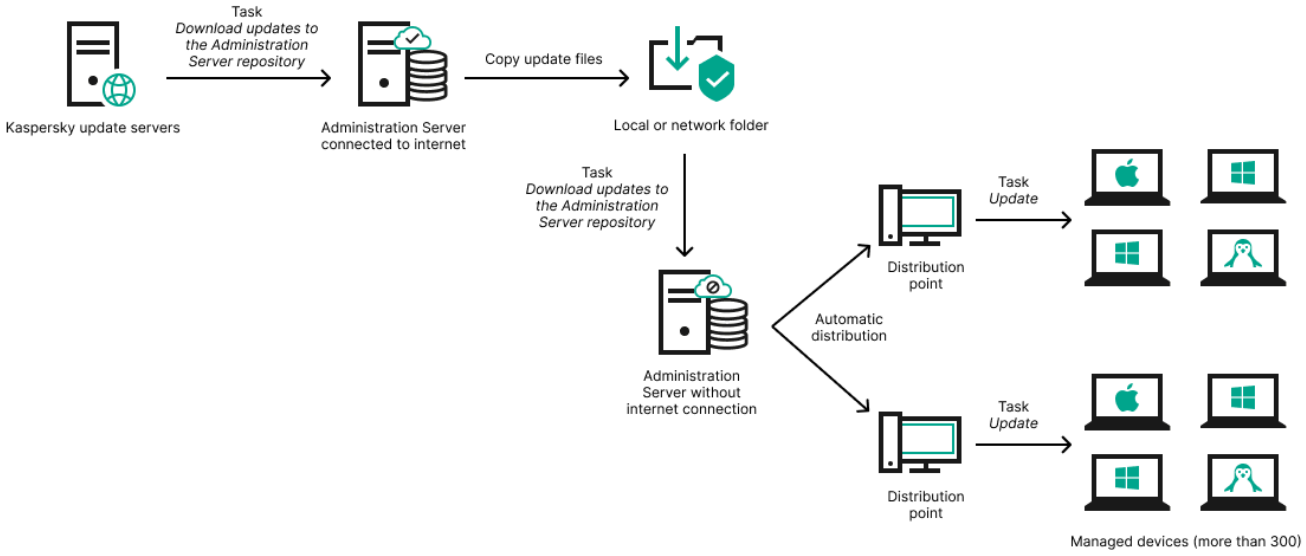
Через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

Если Сервер администрирования не имеет подключения к интернету, вы можете настроить задачу *Загрузка обновлений в хранилище Сервера администрирования* для загрузки обновлений из локальной или сетевой папки. В этом случае требуется время от времени копировать необходимые файлы обновлений в указанную папку. Например, вы можете скопировать необходимые файлы обновления из одного из следующих источников:

- Сервер администрирования, имеющий выход в интернет (см. рис. ниже).

  Так как Сервер администрирования загружает только те обновления, которые запрашиваются приложениями безопасности, наборы приложений безопасности, которыми управляют Серверы администрирования (подключенные и не подключенные к интернету) должны совпадать.

Если Сервер администрирования, который вы используете для загрузки обновлений, имеет версию 13.2 или более раннюю, откройте свойства задачи *Загрузка обновлений в хранилище Сервера администрирования*, а затем включите параметр **Загружать обновления, используя старую схему**.



Обновление через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

- Kaspersky Update Utility

  Так как утилита использует старую схему для загрузки обновлений, откройте свойства задачи *Загрузка обновлений в хранилище Сервера администрирования*, а затем включите параметр **Загружать обновления, используя старую схему**.

Создание задачи Загрузка обновлений в хранилище Сервера администрирования

Задача *Загрузка обновлений в хранилище Сервера администрирования* создается автоматически во время работы мастера первоначальной настройки Kaspersky Security Center. Задача *Загрузка обновлений в хранилище Сервера администрирования* может быть создана в одном экземпляре. Поэтому вы можете создать задачу *Загрузка обновлений в хранилище Сервера администрирования* только в случае, если она была удалена из списка задач Сервера администрирования.

Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования. Список обновлений включает:

- обновления баз и модулей приложений для Сервера администрирования;
- обновления баз и модулей приложений для приложений безопасности "Лаборатории Касперского";
- обновления компонентов Kaspersky Security Center;
- обновления приложений безопасности "Лаборатории Касперского".

После загрузки обновлений их можно распространять на управляемые устройства.

Перед распространением обновлений на управляемые устройства вы можете выполнить задачу *Проверка обновлений*. Это позволяет убедиться, что Сервер администрирования правильно установит загруженные обновления и уровень безопасности не снизится из-за обновлений. Чтобы проверить обновления перед распространением, настройте параметр **Выполнить проверку обновлений** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования*.

*Чтобы создать задачу **Загрузка обновлений в хранилище Сервера администрирования**:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Security Center выберите тип задачи **Загрузка обновлений в хранилище Сервера администрирования**.
4. Укажите название задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
6. Нажмите на кнопку **Создать**.

   Задача будет создана и отобразится в списке задач.
7. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
8. В окне свойств задачи на вкладке **Параметры приложения** укажите следующие параметры:

   - **Источники обновлений**

     В качестве источника обновлений для Сервера администрирования 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 Сервер администрирования взаимодействует с серверами обновлений "Лаборатории Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.

       Выбрано по умолчанию.

     - Главный Сервер администрирования

       Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.

     - Локальная или сетевая папка

Локальная или сетевая папка, которая содержит последние обновления. Сетевая папка может быть FTP-сервером, HTTP-сервером или общим ресурсом SMB. 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".

Если общая папка с обновлениями защищена паролем, включите параметр **Задать учетную запись для доступа к общей папке источника обновлений (если используется)** и введите учетные данные, необходимые для доступа.

- **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.

- Прочие параметры:

  - **Принудительно обновить подчиненные Серверы**

    Если параметр включен, Сервер администрирования будет запускать задачи получения обновлений на подчиненных Серверах администрирования сразу после получения обновлений. Задачи обновления запускаются с использованием источника обновления, который настроен в свойствах задачи на подчиненных Серверах администрирования.

    Если этот параметр выключен, задачи обновления на подчиненных Серверах администрирования начинаются в соответствии с расписанием.

    По умолчанию параметр выключен.

  - **Копировать полученные обновления в дополнительные папки**

    Если флажок установлен, после получения обновлений Сервер администрирования будет копировать обновления в указанные папки. Используйте этот параметр, если хотите управлять вручную обновлениями на вашем устройстве.

    Например, вы можете использовать этот параметр в следующей ситуации: сеть организации содержит несколько независимых подсетей и устройства из каждой подсети не имеют доступ к другой подсети. При этом устройства во всех подсетях имеют доступ к общей сетевой папке. В этом случае для Сервера администрирования в одной из подсетей укажите загрузку обновлений с серверов обновлений "Лаборатории Касперского", включите этот параметр и укажите эту сетевую папку. В задаче загрузка обновлений в хранилище для Сервера администрирования укажите эту же сетевую папку в качестве источника обновлений.

    Если вы выберете копирование загруженных обновлений в локальную папку, необходимо указать на устройстве папку, которая содержит установленный Сервер администрирования. Путь к папке зависит от операционной системы устройства. Поскольку локальная папка расположена на Сервере администрирования с операционной системой Linux, вам нужно указать POSIX-путь, например, /path/to/dir.

    При выборе сетевой папки, расположенной на Сервере администрирования с операционной системой Linux, нужно заранее обеспечить доступ к сетевой папке с устройства, на котором установлен Сервер администрирования, смонтировав папку. Доступ к папке осуществляется с использованием SMB-протокола.

По умолчанию параметр выключен.

- **Не обновлять устройства и подчиненные Серверы администрирования принудительно до окончания копирования**

  Если флажок установлен, задачи получения обновлений клиентскими устройствами и подчиненными Серверами администрирования будут запускаться после окончания копирования обновлений из сетевой папки обновлений в дополнительные папки обновлений.

  Этот флажок должен быть установлен, если клиентские устройства и подчиненные Серверы администрирования скачивают обновления из дополнительных сетевых папок.

  По умолчанию параметр выключен.

- **Состав обновлений**:

  - **Загрузить файлы различий**

    Этот параметр включает функцию загрузки файлов различий.

    По умолчанию параметр выключен.

- **Загружать обновления, используя старую схему**

  Начиная с версии 14, Kaspersky Security Center загружает обновления баз и 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 **Загружать обновления, используя старую схему**. Иначе задача загрузки обновлений завершится ошибкой.

  Например, этот параметр необходимо включить, если в качестве источника обновлений указана локальная или сетевая папка и файлы обновлений в этой папке были загружены одной из следующих приложений:

  - Kaspersky Update Utility

    Эта утилита загружает обновления по старой схеме.

  - Kaspersky Security Center 13.2 или более ранняя версия

    Например, один Сервер администрирования не имеет подключения к интернету. В этом случае можно загружать обновления с помощью второго Сервера администрирования, подключенного к интернету, а затем помещать обновления в локальную или сетевую папку, чтобы использовать ее в качестве источника обновлений для первого Сервера. Если второй Сервер администрирования имеет номер версии 13.2 или ниже, включите параметр **Загружать обновления, используя старую схему** в задаче для первого Сервера администрирования.

  По умолчанию параметр выключен.

- **Выполнить проверку обновлений**

  Если флажок установлен, Сервер администрирования копирует обновления из источника, сохраняет их во временном хранилище и запускает задачу Проверка обновлений, указанную в поле **Задача проверки обновлений**. В случае успешного выполнения этой задачи обновления копируются из временного хранилища в папку общего доступа Сервера администрирования и распространяются на устройства, для которых Сервер администрирования является источником обновлений (запускаются задачи с типом расписания **При загрузке обновлений в хранилище**). Задача загрузки обновлений в хранилище считается завершенной только после завершения задачи *Проверка обновлений*.

  По умолчанию параметр выключен.

9. В окне свойств задачи на вкладке **Расписание** создайте расписания запуска задачи. При необходимости настройте следующие параметры:

   - **Запуск задачи:**

     Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

     - **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.

     - **По дням недели**

       Задача выполняется регулярно, в указанные дни недели, в указанное время.

       По умолчанию задача запускается каждую пятницу в 18:00:00.

     - **Monthly**

       Задача выполняется регулярно, в указанный день месяца, в указанное время.

       В месяцах, у которых нет указанного дня, задача выполняется в последний день.

       По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

     - **Ежемесячно, в указанные дни выбранных недель**

       Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

       По умолчанию 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 задач**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать автоматическую случайную задержку запуска задачи в интервале**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

- **Остановить, если задача выполняется дольше**

  По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

  Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

  По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

10. Нажмите на кнопку **Сохранить**.

    Задача создана и настроена.

В результате выполнения задачи *Загрузка обновлений в хранилище Сервера администрирования* обновления баз и модули приложений копируются с источника обновлений и размещаются в папке общего доступа Сервера администрирования. Если задача создается для группы администрирования, то она распространяется только на Агенты администрирования, входящие в указанную группу администрирования.

Из папки общего доступа обновления распространяются на клиентские устройства и подчиненные Серверы администрирования.

Проверка полученных обновлений

Перед установкой обновлений на управляемые устройства вы можете сначала проверить их на работоспособность и ошибки с помощью задачи *Проверка обновлений*. Задача *Проверка обновлений* выполняется автоматически в рамках задачи *Загрузка обновлений в хранилище Сервера администрирования*. Сервер администрирования загружает обновления с источника, сохраняет их во временном хранилище и запускает задачу *Проверка обновлений*. В случае успешного выполнения этой задачи обновления копируются из временного хранилища в папку общего доступа Сервера администрирования. Обновления распространяются на клиентские устройства, для которых Сервер администрирования является источником обновления.

Если по результатам выполнения задачи *Проверка обновлений* размещенные во временном хранилище обновления признаны некорректными или задача завершается с ошибкой, копирование обновлений в папку общего доступа не производится. На Сервере администрирования остается предыдущий набор обновлений. Запуск задач с типом расписания **При загрузке обновлений в хранилище** также не выполняется. Эти операции выполняются при следующем запуске задачи *Загрузка обновлений в хранилище Сервера администрирования*, если проверка нового набора обновлений завершится успешно.

Набор обновлений считается некорректным, если хотя бы на одном из тестовых устройств выполняется одно из следующих условий:

- произошла ошибка выполнения задачи обновления;
- после применения обновлений изменился статус постоянной защиты приложения безопасности;
- в ходе выполнения задачи проверки по требованию был найден зараженный объект;
- произошла ошибка функционирования приложения "Лаборатории Касперского".

Если ни одно из перечисленных условий ни на одном из тестовых устройств не выполняется, набор обновлений признается корректным и задача *Проверка обновлений* считается успешно выполненной.

Прежде чем приступить к созданию задачи *Проверка обновлений*, выполните предварительные условия:

1. Создайте группу администрирования с несколькими тестовыми устройствами. Эта группа понадобится вам для проверки обновлений.

   В качестве тестовых устройств рекомендуется использовать хорошо защищенные устройства с наиболее распространенной в сети организации программной конфигурацией. Такой подход повышает качество и вероятность обнаружения вирусов при проверке, а также минимизирует риск ложных срабатываний. При нахождении вирусов на тестовых устройствах задача *Проверка обновлений* считается завершившейся неудачно.

2. Создайте задачи обновления и поиска вредоносного ПО для какого-нибудь приложения, которое поддерживает Kaspersky Security Center, например, Kaspersky Endpoint Security для Windows или Kaspersky Security для Windows Server.При создании задач обновления и поиска вредоносного ПО укажите группу администрирования с тестовыми устройствами.

   Задача *Проверка обновлений* последовательно запускает задачи обновления и поиска вредоносного ПО на тестовых устройствах, чтобы убедиться, что все обновления актуальны. Также при создании задачи *Проверка обновлений* необходимо указать задачи обновления и поиска вредоносного ПО.

3. Создайте задачу *Загрузка обновлений в хранилище Сервера администрирования*.

Чтобы Kaspersky Security Center проверял полученные обновления перед распространением их на клиентские устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на название задачи **Загрузка обновлений в хранилище Сервера администрирования**.
3. В открывшемся окне свойств задачи выберите вкладку **Параметры приложения** и включите параметр **Выполнить проверку обновлений**.
4. Если задача *Проверка обновлений* существует, нажмите на кнопку **Выберите задачу**. В открывшемся окне выберите задачу *Проверка обновлений* в группе администрирования с тестовыми устройствами.

5. Если вы не создавали задачу *Проверка обновлений* ранее, выполните следующие действия:

   a. Нажмите на кнопку **Новая задача**.

   b. В открывшемся мастере создания задачи укажите имя задачи, если вы хотите изменить предустановленное имя.

   c. Выберите созданную ранее группу администрирования с тестовыми устройствами.

   d. Выберите задачу обновления нужного приложения, поддерживаемого Kaspersky Security Center, а затем выберите задачу поиска вредоносного ПО.

   После этого появляются следующие параметры. Рекомендуется оставить их включенными:

   - **Перезагружать устройство после обновления баз**

     После обновления антивирусных баз на устройстве рекомендуется перезагрузить устройство.

     По умолчанию параметр включен.

   - **Проверять статус постоянной защиты после обновления баз и перезапуска устройства**

     Если этот параметр включен, задача *Проверка обновлений* проверяет, актуальны ли обновления, загруженные в хранилище Сервера администрирования, и не снизился ли уровень защиты после обновления антивирусных баз и перезагрузки устройства.

     По умолчанию параметр включен.

   e. Укажите учетную запись, под которой будет запущена задача *Проверка обновлений*. Вы можете использовать свою учетную запись и оставить включенным параметр **Учетная запись по умолчанию**. Кроме того, можно указать, что задача должна выполняться под другой учетной записью, имеющей необходимые права доступа. Для этого выберите параметр **Задать учетную запись** и введите учетные данные этой учетной записи.

6. Закройте окно свойств задачи *Загрузка обновлений в хранилище Сервера администрирования*, нажав на кнопку **Сохранить**.

Автоматическая проверка обновлений включена. Теперь вы можете запустить задачу *Загрузка обновлений в хранилище Сервера администрирования*, и она начнется с проверки обновлений.

Создание задачи загрузки обновлений в хранилища точек распространения

Задача *Загрузка обновлений в хранилища точек распространения* работает только с точками распространения под управлением Windows. Точки распространения под управлением Linux или macOS не могут загружать обновления с серверов обновлений "Лаборатории Касперского". Если хотя бы одно устройство с операционной системой Linux или macOS находится в области действия задачи, задача будет иметь статус *Сбой*. Даже если задача успешно завершена на всех устройствах с операционной системой Windows, она вернет ошибку на остальных устройствах.

Вы можете создать задачу *Загрузка обновлений в хранилища точек распространения* для группы администрирования. Такая задача будет выполняться для точек распространения, входящих в указанную группу администрирования.

Вы можете использовать эту задачу, например, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.

Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилища точек распространения. Список обновлений включает:

- обновления баз и модулей приложений для приложений безопасности "Лаборатории Касперского";
- обновления компонентов Kaspersky Security Center;
- обновления приложений безопасности "Лаборатории Касперского".

После загрузки обновлений их можно распространять на управляемые устройства.

Если точки распространения подключаются к интернету с помощью прокси-сервера, вам нужно указать соответствующие параметры политики Агента администрирования.

*Чтобы создать задачу **Загрузка обновлений в хранилища точек распространения** для выбранной группы администрирования:*

1. в главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Security Center выберите в поле **Тип задачи** выберите **Загрузка обновлений в хранилища точек распространения**.
4. Укажите 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. На шаге **Завершение создания задачи**, если вы хотите изменить параметры задачи по умолчанию, включите параметр **Открыть окно свойств задачи после ее создания**. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
7. Нажмите на кнопку **Создать**.

   Задача будет создана и отобразится в списке задач.
8. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
9. На вкладке **Параметры приложения** окна свойств задачи укажите следующие параметры:

   - **Источники обновлений**

     В качестве источника обновлений для точки распространения могут быть использованы следующие ресурсы:

     - Серверы обновлений "Лаборатории Касперского"

       HTTP-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложения.

По умолчанию этот вариант выбран.

- Локальная или сетевая папка

  Локальная или сетевая папка, которая содержит последние обновления. 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.

- **Загрузить файлы различий**

  Этот параметр включает функцию загрузки файлов различий.

  По умолчанию параметр выключен.

- **Загружать обновления, используя старую схему**

  Начиная с версии 14, Kaspersky Security Center загружает обновления баз и 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 **Загружать обновления, используя старую схему**. Иначе задача загрузки обновлений завершится ошибкой.

  Например, этот параметр необходимо включить, если в качестве источника обновлений указана локальная или сетевая папка и файлы обновлений в этой папке были загружены одной из следующих 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 **Загружать обновления, используя старую схему** в задаче *Загружать обновления в хранилища точек распространения*.

  По умолчанию параметр выключен.

10. Создайте расписания запуска задачи. При необходимости настройте следующие параметры:

- **Запуск задачи**

  Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

  - **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.

  - **По дням недели**

    Задача выполняется регулярно, в указанные дни недели, в указанное время.

    По умолчанию задача запускается каждую пятницу в 18:00:00.

  - **Ежемесячно**

    Задача выполняется регулярно, в указанный день месяца, в указанное время.

    В месяцах, у которых нет указанного дня, задача выполняется в последний день.

    По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

  - **Ежемесячно, в указанные дни выбранных недель**

    Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

    По умолчанию 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.

Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center

Обновления и патчи для Сервера администрирования могут быть установлены только после получения явного одобрения администратором.

Автоматическая установка обновлений для компонентов Kaspersky Security Center 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 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. Вы можете включить автоматическую установку позже с помощью политики.

Чтобы выключить автоматическую установку обновлений для компонентов Kaspersky Security Center 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 откройте 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. Вы можете включить автоматическую установку позже с помощью политики.

Если при установке Агента администрирования на устройство флажок был установлен (снят), 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 с помощью политики Агента администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства) → Политики и профили политик**.
2. Нажмите на политику Агента администрирования.
3. В окне свойств политики откройте вкладку **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. Установите замок (🔒) для этого переключателя.

   Политика применится к выбранным устройствам, и автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center 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 **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Endpoint Security для Windows выберите подтип задачи **Обновление**.
4. Укажите название задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите область действия задачи.
6. Укажите группу администрирования, выборку устройств или устройства, к которым применяется задача.
7. На шаге **Завершение создания задачи**, если вы хотите изменить параметры задачи по умолчанию, включите параметр **Открыть окно свойств задачи после ее создания**. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
8. Нажмите на кнопку **Создать**.

   Задача будет создана и отобразится в списке задач.
9. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
10. В окне свойств задачи обновления на вкладке **Параметры приложения** укажите локальный или мобильный режим:

    - **Локальный режим**: между устройством и Сервером администрирования установлена связь.
    - **Мобильный режим**: между устройством и Kaspersky Security Center не установлена связь (например, если устройство не подключено к интернету).
11. Включите источники обновлений, которые вы хотите использовать для обновления баз и модулей приложения для Kaspersky Endpoint Security для Windows. Если требуется изменить положение источников обновлений в списке, используйте кнопки **Вверх** и **Вниз**. Если включено несколько источников обновлений, Kaspersky Endpoint Security для Windows пытается подключиться к ним один за другим, начиная с верхней части списка, и выполняет задачу обновления, извлекая пакет обновления из первого доступного источника.
12. Включите параметр **Устанавливать одобренные обновления модулей приложений**, чтобы загружать и устанавливать обновления модулей приложений вместе с базами приложений.

Если параметр включен, то Kaspersky Endpoint Security для Windows уведомляет пользователя о доступных обновлениях модулей приложения и во время выполнения задачи обновления включает обновления модулей приложения в пакет обновлений. Kaspersky Endpoint Security для Windows устанавливает только те обновления, для которых вы установили статус *Одобрено*; обновления будут установлены локально через интерфейс приложения или через Kaspersky Security Center.

Вы также можете включить параметр **Автоматически устанавливать критические обновления модуля приложения**. При наличии обновлений модулей приложения Kaspersky Endpoint Security для Windows устанавливает обновления со статусом *Предельный* автоматически; остальные обновления модулей приложения – после одобрения их установки администратором.

Если обновление модулей приложения предполагает ознакомление и согласие с положениями Лицензионного соглашения и Политики конфиденциальности, то приложение устанавливает обновление после согласия пользователя с положениями Лицензионного соглашения и Политики конфиденциальности.

13. Установите флажок **Копировать обновления в папку**, чтобы приложение сохраняло загруженные обновления в папку, а затем укажите путь к папке.

14. Задайте расписание запуска задачи. Чтобы обеспечить своевременное обновление, рекомендуется выбрать вариант **При загрузке обновлений в хранилище**.

15. Нажмите на кнопку **Сохранить**.

При выполнении задачи **Обновление** приложение отправляет запросы серверам обновлений "Лаборатории Касперского".

Некоторые обновления требуют установки последних версий плагинов управляемых приложений.

Одобрение и отклонение обновлений программного обеспечения

Параметры задачи установки обновлений могут требовать одобрения обновлений, которые должны быть установлены. Вы можете подтверждать обновления, которые необходимо установить, и отклонять обновления, которые не должны быть установлены.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом установить эти обновления на клиентские устройства.

Одобрение и отклонение обновлений доступно только для Агента администрирования и управляемых приложений, установленных на клиентских устройствах под управлением Windows. Бесшовное обновление Сервера администрирования, Kaspersky Security Center Web Console и веб-плагинов управления не поддерживается. Для обновления этих компонентов вам необходимо скачать их последние версии с сайта "Лаборатории Касперского" и установить их вручную.

Чтобы подтвердить или отменить одно или несколько обновлений:

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения "Лаборатории Касперского"** → **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. 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*.

Обновления, для которых вы установили статус *Одобрено*, помещаются в очередь на установку.

Обновления, для которых вы установили статус *Отклонено*, деинсталлируются (если это возможно) с устройств, на которые они были ранее установлены. Также они не будут установлены на устройства позже.

Некоторые обновления для приложений "Лаборатории Касперского" невозможно деинсталлировать. Если вы установили для них статус *Отклонено*, Kaspersky Security Center не будет деинсталлировать эти обновления с устройств, на которые они были установлены ранее. Такие обновления никогда не будут установлены на устройства в будущем.

Если вы устанавливаете статус *Отклонено* для обновлений стороннего программного обеспечения, то эти обновления не будут устанавливаться на те устройства, для которых они были запланированы к установке, но еще не были установлены. Обновления останутся на тех устройствах, на которые они уже были установлены. Если вам потребуется удалить обновления, вы можете сделать это вручную локально.

Обновление Сервера администрирования

Вы можете установить обновления Сервера администрирования с помощью Мастер обновления Сервера администрирования.

Чтобы установить обновления Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Операции → Приложения "Лаборатории Касперского" → Обновления**.

2. Запустите Мастер обновления Сервера администрирования одним из следующих способов:

   - Нажмите на имя обновления Сервера администрирования в списке обновлений и в открывшемся окне перейдите по ссылке **Запустить мастер обновления Сервера администрирования**.

   - Перейдите по ссылке **Запустить мастер обновления Сервера администрирования** в поле уведомления в верхней части окна приложения.

3. Чтобы указать, когда устанавливать обновление, в окне Мастер обновления Сервера администрирования выберите один из следующих вариантов:

   - **Установить сейчас**. Выберите этот вариант, если вы хотите установить обновления сейчас.
   - **Отложить установку**. Выберите этот вариант, если вы хотите установить обновления позже. В этом случае будет отображаться уведомление об этом обновлении.
   - **Игнорировать это обновление**. Выберите этот вариант, если вы не хотите устанавливать обновление и не хотите получать уведомления об этом обновлении.

4. Если вы хотите создать резервную копию Сервера администрирования перед установкой обновления, выберите параметр **Сделать резервную копию Сервера администрирования перед установкой обновления**.

5. Нажмите на кнопку **ОК**, чтобы закрыть окно мастера.

В процессе резервного копирования прерывается процесс установки обновлений.

Включение и выключение офлайн-модели получения обновлений

Не рекомендуется выключать офлайн-модель получения обновлений. Выключение может привести к сбоям в доставке обновлений на устройства. В некоторых случаях специалисты Службы технической поддержки "Лаборатории Касперского" могут рекомендовать вам выключить параметр **Загружать обновления и антивирусные базы с Сервера администрирования заранее**. Тогда вам нужно будет убедиться, что задача загрузки обновлений в хранилище для приложений "Лаборатории Касперского" настроена.

Чтобы включить или выключить офлайн-модель получения обновлений для группы администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.

2. Нажмите на кнопку **Группы**.

3. В списке групп администрирования выберите группу администрирования, для которой требуется включить офлайн-модель получения обновлений.

4. Нажмите на политику Агента администрирования.

   Откроется окно свойств политики Агента администрирования.

   По умолчанию параметры дочерней политики наследуют параметры родительской политики и не могут быть изменены. Если политика, которую вы хотите изменить, унаследована, то вам нужно создать политику для Агента администрирования в требуемой группе администрирования. В созданной политике вы можете изменить параметры, которые не заблокированы в родительской политике.

5. В окне **Параметры приложения** выберите раздел **Управление патчами и обновлениями**.

6. Включите или выключите параметр **Загружать обновления и антивирусные базы с Сервера администрирования заранее (рекомендуется)**, чтобы включить или выключить офлайн-модель получения обновлений соответственно.

   По умолчанию офлайн-модель получения обновлений включена.

В результате офлайн-модель получения обновлений будет включена или выключена.

Обновление баз и модулей приложений "Лаборатории Касперского" на автономных устройствах

Обновление баз и модулей приложений "Лаборатории Касперского" на управляемых устройствах является важной задачей для обеспечения защиты устройств от вирусов и других угроз. Администратор обычно настраивает регулярное обновление с помощью хранилища Сервера администрирования или хранилищ точек распространения.

Когда вам необходимо обновить базы данных и модули приложений на устройстве (или группе устройств), которое не подключено к Серверу администрирования (главному или подчиненному), точке распространения или интернету, вам необходимо использовать альтернативные источники обновлений, такие как FTP-сервер или локальная папка. В этом случае вам нужно доставить файлы необходимых обновлений с помощью запоминающего устройства, такого как флеш-накопитель или внешний жесткий диск.

Вы можете скопировать требуемые обновления с:

- Сервера администрирования.

  Чтобы хранилище Сервера администрирования содержало обновления, необходимые для приложения безопасности, установленного на автономном устройстве, по крайней мере на одном из управляемых сетевых устройств должно быть установлено это приложение безопасности. Это приложение должно быть настроено на получение обновлений из хранилища Сервера администрирования с помощью задачи Загрузка обновлений в хранилище Сервера администрирования.

- Любого устройства, на котором установлено такое же приложение безопасности и настроено получение обновлений из хранилища Сервера администрирования, хранилища точки распространения или напрямую с серверов обновлений "Лаборатории Касперского".

Ниже приведен пример настройки обновлений баз и модулей приложений путем копирования их из хранилища Сервера администрирования.

Чтобы обновить базы данных и модули приложений "Лаборатории Касперского" на автономных устройствах:

1. Подключите съемный диск к устройству, на котором установлен Сервер администрирования.

2. Скопируйте файлы обновлений на съемный диск.

   По умолчанию обновления расположены: \\<server name>\KLSHARE\Updates.

   Также вы можете настроить в Kaspersky Security Center регулярное копирование обновлений в выбранную вами папку. Для этого используйте параметр **Копировать полученные обновления в дополнительные папки** в свойствах задачи Загрузка обновлений в хранилище Сервера администрирования. Если вы укажете папку, расположенную на запоминающем устройстве или внешнем жестком диске, в качестве папки назначения для этого параметра, это запоминающее устройство всегда будет содержать последнюю версию обновлений.

3. На автономных устройствах настройте 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.

Резервное копирование и восстановление веб-плагинов

Kaspersky Security Center Web Console позволяет создавать резервную копию данных текущего состояния веб-плагина, чтобы впоследствии можно было восстановить сохраненное состояние. Например, вы можете создать резервную копию данных веб-плагина перед его обновлением до более новой версии. После обновления, если более новая версия не соответствует вашим требованиям или ожиданиям, вы можете восстановить предыдущую версию веб-плагина из резервной копии данных.

Для резервного копирования данных веб-плагинов:

1. В главном меню перейдите в раздел **Параметры** → **Веб-плагины**.

2. В разделе **Веб-плагины** выберите веб-плагины, для которых требуется создать резервную копию данных, а затем нажмите на кнопку **Создать резервную копию данных**.

   Резервное копирование данных выбранных веб-плагинов. Вы можете просмотреть созданные резервные копии данных в разделе **Резервные копии данных**.

Чтобы восстановить веб-плагин из резервной копии данных:

1. В главном меню перейдите в раздел **Параметры** → **Резервные копии данных**.

2. В разделе **Резервные копии данных** выберите резервную копию данных веб-плагина, которую вы хотите восстановить, а затем нажмите на кнопку **Восстановить из резервной копии данных**.

   Веб-плагин восстанавливается из выбранной резервной копии данных.

Настройка точек распространения и шлюзов соединений

Структура групп администрирования в Kaspersky Security Center выполняет следующие функции:

- Задание области действия политик.

  Существует альтернативный способ применения нужных наборов параметров на устройствах с помощью *профилей политик*. В этом случае область действия 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, виртуальным и подчиненным Серверам администрирования.
- Назначение точек распространения.

При построении структуры групп администрирования следует учитывать топологию сети организации для оптимального назначения точек распространения. Оптимальное распределение точек распространения позволяет уменьшить сетевой трафик внутри сети организации.

В зависимости от организационной структуры организации и топологии сетей можно выделить следующие типовые конфигурации структуры групп администрирования:

- Один офис.
- Множество небольших изолированных офисов.

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

Типовая конфигурация точек распространения: один офис

В типовой конфигурации "один офис" все устройства находятся в сети организации и "видят" друг друга. Сеть организации может состоять из нескольких выделенных частей (сетей или сегментов сети), связанных узкими каналами.

Возможны следующие способы построения структуры групп администрирования:

- Построение структуры групп администрирования с учетом топологии сети. Структура групп администрирования не обязательно должна точно отражать топологию сети. Достаточно того, чтобы выделенным частям сети соответствовали какие-либо группы администрирования. Можно использовать автоматическое назначение точек распространения, либо назначать точки распространения вручную.
- Построение структуры групп администрирования, не отражающей топологию сети. В этом случае следует отключить автоматическое назначение точек распространения и в каждой выделенной части сети назначить одно или несколько устройств точками распространения на корневую группу администрирования, например, на группу **Управляемые устройства**. Все точки распространения окажутся на одном уровне и будут иметь одинаковую область действия "все устройства сети организации". Каждый Агент администрирования будет подключаться к той точке распространения, маршрут к которой является самым коротким. Маршрут к точке распространения можно определить с помощью утилиты tracert.

Типовая конфигурация точек распространения: множество небольших удаленных офисов

Этой типовой конфигурации соответствует множество небольших удаленных офисов, возможно, связанных с главным офисом через интернет. Каждый из удаленных офисов находится за NAT, то есть подключение из одного удаленного офиса в другой невозможно – офисы изолированы друг от друга.

Конфигурацию следует обязательно отразить в структуре групп администрирования: для каждого из удаленных офисов следует создать отдельную группу администрирования (группы **Офис 1**, **Офис 2** на рисунке ниже).



Удаленные офисы отражены в структуре групп администрирования

На каждую группу администрирования, соответствующую офису, нужно назначить одну или несколько точек распространения. Точками распространения нужно назначать устройства удаленного офиса, имеющие достаточно места на диске. Устройства, размещенные, например, в группе **Офис 1**, будут обращаться к точкам распространения, назначенным на группу администрирования **Офис 1**.

Если некоторые пользователи физически перемещаются между офисами с ноутбуками, нужно в каждом удаленном офисе дополнительно к упомянутым выше точкам распространения выбрать два и или более устройств и назначить их точками распространения на группу администрирования верхнего уровня (группа **Корневая группа для офисов** на рисунке выше).

Ноутбук, находившийся в группе администрирования **Офис 1**, но физически перемещенный в офис, соответствующий группе **Офис 2**. После перемещения Агент администрирования на ноутбуке попытается обратиться к точкам распространения, назначенным на группу **Офис 1**, но эти точки распространения окажутся недоступны. Тогда Агент администрирования начнет обращаться к точкам распространения, назначенным на группу **Корневая группа для офисов**. Так как удаленные офисы изолированы друг от друга, то из всех точек распространения, назначенных на группу администрирования **Корневая группа для офисов**, успешными будут лишь обращения к точкам распространения, назначенным на группу **Офис 2**. То есть ноутбук, оставаясь в группе администрирования, соответствующей своему исходному офису, будет, тем не менее, использовать точку распространения того офиса, в котором в данный момент находится физически.

О назначении точек распространения

Вы можете назначить управляемое устройство в качестве точки распространения вручную или автоматически.

Если вы назначаете управляемое устройство в качестве точки распространения вручную, вы можете выбрать любое устройство в своей сети.

Если вы назначаете точки распространения автоматически, Kaspersky Security Center может выбрать только то управляемые устройства, которые соответствует следующим условиям:

- Устройство должно иметь не менее 50 ГБ свободного места на диске.
- Управляемое устройство подключается к Kaspersky Security Center напрямую (не через шлюз).
- Управляемое устройство не является ноутбуком.

> Если в вашей сети нет устройств, соответствующих заданным условиям, Kaspersky Security Center не будет автоматически назначать какое-либо устройство точкой распространения.

Автоматическое назначение точек распространения

Рекомендуется назначать точки распространения автоматически. В этом случае Kaspersky Security Center будет сам выбирать, какие устройства назначать точками распространения.

Устройства с операционной системой Microsoft Windows на Arm не могут выступать в роли точек распространения.

Чтобы назначить точки распространения автоматически:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.

3. Выберите параметр **Автоматически назначать точки распространения**.

   Если автоматическое назначение устройств точками распространения включено, невозможно вручную настраивать параметры точек распространения, а также изменять список точек распространения.

4. Нажмите на кнопку **Сохранить**.

В результате Сервер администрирования будет автоматически назначать точки распространения и настраивать их параметры.

Назначение точек распространения вручную

Kaspersky Security Center позволяет вручную назначать устройства точками распространения.

Рекомендуется назначать точки распространения автоматически. В этом случае Kaspersky Security Center будет сам выбирать, какие устройства назначать точками распространения. Однако если вы по какой-то причине хотите отказаться от автоматического назначения точек распространения (например, если вы хотите использовать специально выделенные серверы), вы можете назначать точки распространения вручную, предварительно рассчитав их количество и конфигурацию точек распространения.

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

Устройства с операционной системой Microsoft Windows Arm не могут выступать в роли точек распространения.

Чтобы вручную назначить устройство точкой распространения:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.

3. Выберите параметр **Вручную назначать точки распространения**.

4. Нажмите на кнопку **Назначить**.

5. Выберите устройство, которое вы хотите сделать точкой распространения.

   При выборе устройства учитывайте особенности работы точек распространения и требования к устройству, которое выполняет роль точки распространения.

6. Выберите группу администрирования, которую вы хотите включить в область действия выбранной точки распространения.

7. Нажмите на кнопку **OK**.

   Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.

8. Нажмите на добавленную точку распространения в списке, чтобы открыть окно ее свойств.

9. В окне свойств настройте параметры точки распространения:

   - В разделе **Общие** укажите параметр взаимодействия точки распространения с клиентскими устройствами:

     - **SSL-порт**

       Номер SSL-порта, по которому осуществляется защищенное подключение клиентских устройств к точке распространения с использованием протокола SSL.

       По умолчанию номер порта – 13000.

     - **Использовать многоадресную IP-рассылку**

       Если параметр включен, для автоматического распространения инсталляционных пакетов на клиентские устройства в пределах группы будет использоваться многоадресная IP-рассылка.

       Многоадресная IP-рассылка уменьшает время, необходимое для установки приложений из инсталляционного пакета на группу клиентских устройств, но увеличивает время установки при установке приложения на одно клиентское устройство.

     - **Адрес IP-рассылки**

       IP-адрес, на который будет выполняться многоадресная рассылка. IP-адрес можно задать в диапазоне 224.0.0.0 – 239.255.255.255

       По умолчанию Kaspersky Security Center автоматически назначает уникальный IP-адрес многоадресной рассылки в заданном диапазоне.

     - **Номер порта IP-рассылки**

       Номер порта многоадресной рассылки.

Номер порта по умолчанию – 15001. Если в качестве точки распространения указано устройство, на котором установлен Сервер администрирования, то для подключения с использованием SSL-протокола по умолчанию используется порт 13001.

- **Адрес точки распространения для удаленных устройств**

  Сетевой адрес, через который удаленные устройства подключаются к точке распространения.

- **Распространять обновления**

  Обновления распространяются на управляемые устройства из следующих источников:

  - Эта точка распространения, если этот параметр включен.
  - Другие точки распространения, Сервер администрирования или серверы обновлений "Лаборатории Касперского", если параметр выключен.

  Если вы используете точки распространения для распространения обновлений, вы можете сэкономить трафик, так как уменьшите количество загрузок. Также вы можете снизить нагрузку на Сервер администрирования и перераспределить нагрузку между точками распространения. Вы можете вычислить количество точек распространения в вашей сети для оптимизации трафика и нагрузки.

  Если вы выключите этот параметр, количество загрузок обновлений и нагрузка на Сервер администрирования могут увеличиться. По умолчанию параметр включен.

- **Распространять инсталляционные пакеты**

  Инсталляционные пакеты распространяются на управляемые устройства из следующих источников:

  - Эта точка распространения, если этот параметр включен.
  - Другие точки распространения, Сервер администрирования или серверы обновлений "Лаборатории Касперского", если параметр выключен.

  Если вы используете точки распространения для распространения инсталляционных пакетов, вы можете сэкономить трафик, так как уменьшите количество загрузок. Также вы можете снизить нагрузку на Сервер администрирования и перераспределить нагрузку между точками распространения. Вы можете вычислить количество точек распространения в вашей сети для оптимизации трафика и нагрузки.

  Если вы выключите этот параметр, количество загрузок инсталляционных пакетов и нагрузка на Сервер администрирования могут увеличиться. По умолчанию параметр включен.

- **Запустить push-сервер**

  В Kaspersky Security Center точка распространения может работать как push-сервер для устройств, которые управляются по мобильному протоколу, и для устройств под управлением Агента администрирования. Например, push-сервер должен быть включен, если вы хотите включить принудительную синхронизацию устройств с KasperskyOS с Сервером администрирования. Push-сервер имеет ту же область управляемых устройств, что и точка распространения, на которой включен push-сервер. Если у вас есть несколько точек распространения, назначенных для одной и той же группы администрирования, вы можете включить извещающий сервер на каждой них. В этом случае Сервер администрирования распределяет нагрузку между точками распространения.

- **Порт push-сервера**

  Номер порта push-сервера. Вы можете указать номер любого свободного порта.

- В разделе **Область действия** укажите область, на которую точка распространения распространяет обновления (группы администрирования и/или сетевое местоположение).

  Только устройства под управлением операционной системы Windows могут определять свое сетевое местоположение. Определение сетевого местоположения недоступно для устройств под управлением других операционных систем.

- Если точка распространения работает на машине, отличной от Сервера администрирования, в разделе **Источник обновлений** можно выбрать источник обновлений для точки распространения:

  - **Источник обновлений**

    Выберите источник обновлений для точки распространения:

    - Чтобы точка распространения получала обновления с Сервера администрирования, выберите вариант **Получить с Сервера администрирования**.

    - Чтобы разрешить точке распространения получать обновления с помощью задачи, выберите **Использовать задачу загрузки обновлений в хранилище** и укажите задачу *Загружать обновления в хранилища точек распространения*.

      - Если такая задача уже существует для устройства, выберите задачу в списке.

      - Если такой задачи для устройства еще нет, перейдите по ссылке **Создать задачу** для создания задачи. Запустится мастер создания задачи. Следуйте далее указаниям мастера.

  - **Загрузить файлы различий**

    Этот параметр включает функцию загрузки файлов различий.

    По умолчанию параметр включен.

- Если ваши точки распространения используют прокси-сервер для подключения к интернету, в подразделе **Параметры подключения к интернету** вы можете указать следующие параметры:

  - **Использовать прокси-сервер**

    Если этот флажок установлен, для подключения точек распространения к серверу обновлений "Лаборатории Касперского" используется прокси-сервер в интернете. Вы можете настроить подключение к прокси-серверу в полях ввода.

    По умолчанию флажок снят.

  - **Адрес прокси-сервера**

    Адрес прокси-сервера.

  - **Номер порта**

    Номер порта, по которому будет выполняться подключение.

  - **Не использовать прокси-сервер для локальных адресов**

    Если параметр включен, то при подключении к устройствам в локальной сети не используется прокси-сервер.

    По умолчанию параметр выключен.

- **Аутентификация на прокси-сервере**

  Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  По умолчанию флажок снят.

- **Имя пользователя**

  Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.

- **Пароль**

  Пароль учетной записи, от имени которой будет запускаться задача.

- В разделе **Прокси-сервер KSN** вы можете настроить приложение так, чтобы точка распространения использовалась для пересылки KSN запросов от управляемых устройств.

  - **Включить прокси-сервер KSN на стороне точки распространения**

    Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

    Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского".

    По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены в окне свойств Сервера администрирования.

    Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

  - **Пересылать KSN запрос Серверу администрирования**

    Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

    По умолчанию параметр включен.

  - **Доступ к облачной службе KSN/KPSN непосредственно через интернет**

    Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или KPSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или KPSN.

    Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к KPSN. Если вы хотите перенастроить точки распространения для отправки запросов KSN в KPSN, включите параметр **Пересылать KSN запрос Серверу администрирования** для каждой точки распространения.

    Точки распространения с установленным Агентом администрирования версии 12 (и выше) могут напрямую обращаться к KPSN.

  - **Игнорировать параметры прокси-сервера для подключения к KPSN**

    Установите этот флажок, если параметры прокси-сервера настроены в свойствах точки распространения или политики Агента администрирования, но ваша архитектура сети требует, чтобы вы использовали KPSN напрямую. В противном случае запрос от управляемого приложения не будет передан в KPSN.

Это параметр доступен, если вы выбрали параметр **Доступ к облачной службе KSN/KPSN непосредственно через интернет**.

- **Порт**

  Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.

- **Использовать UDP-порт**

  Чтобы управляемые устройства подключались к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и укажите номер UDP-порта. По умолчанию параметр включен.

- **UDP-порт**

  Номер UDP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

- Если точка распространения работает на машине, отличной от Сервера администрирования, в разделе **Шлюз соединения** можно настроить точку распространения как шлюз соединения для экземпляров Агента администрирования и Сервером администрирования:

  - **Шлюз соединения**

    Если прямое соединение между Сервером администрирования и Агентами администрирования не может быть установлено из-за организации вашей сети, вы можете использовать точку распространения в качестве шлюза соединения между Сервером администрирования и Агентами администрирования.

    Включите этот параметр, если требуется, чтобы точка распространения выполняла роль шлюза соединения между Агентами администрирования и Сервером администрирования. По умолчанию параметр выключен.

  - **Установить соединение с шлюзом со стороны Сервера администрирования (если шлюз размещен в демилитаризованной зоне)**

    Если Сервер администрирования находится за пределами демилитаризованной зоны (DMZ), в локальной сети, Агенты администрирования, установленные на удаленных устройствах, не могут подключаться к Серверу администрирования. Вы можете использовать точку распространения в качестве шлюза соединения с обратным подключением (Сервер администрирования устанавливает соединение с точкой распространения).

    Включите этот параметр, если требуется подключить Сервер администрирования к шлюзу соединения в демилитаризованной зоне.

  - **Открыть локальный порт для Kaspersky Security Center Web Console**

    Включите этот параметр, если вам нужен шлюз соединения в демилитаризованной зоне, чтобы открыть порт для Web Console, находящейся в демилитаризованной зоне или в интернете. Укажите номер порта, который будет использоваться для подключения Web Console к точке распространения. По умолчанию установлен порт 13299.

    Это параметр доступен, если включен параметр **Установить соединение с шлюзом со стороны Сервера администрирования (если шлюз размещен в демилитаризованной зоне)**.

При подключении мобильных устройств к Серверу администрирования через точку распространения, выполняющую роль шлюза соединения, вы можете включить следующие параметры:

- **Открыть порт для мобильных устройств (SSL-аутентификация только Сервера администрирования)**

  Включите этот параметр, если требуется, чтобы шлюз соединения открывал порт для мобильных устройств, и укажите номер порта, который мобильные устройства будут использовать для подключения к точке распространения. По умолчанию установлен порт 13292. Мобильное устройство проверит сертификат Сервера администрирования. При установке соединения только Сервер администрирования выполняет аутентификацию.

- **Открыть порт для мобильных устройств (двусторонняя SSL-аутентификация)**

  Включите этот параметр, если требуется, чтобы шлюз соединения открывал порт, который будет использоваться для двусторонней аутентификации Сервера администрирования и мобильных устройств. Мобильное устройство проверит сертификат Сервера администрирования, а Сервер администрирования проверит сертификат мобильного устройства. Задайте следующие параметры:

  - Номер порта, который мобильные устройства будут использовать для подключения к точке распространения. По умолчанию установлен порт 13293.

  - Имена DNS-доменов шлюза соединения, которые будут использоваться мобильными устройствами. Разделяйте имена доменов запятыми. Указанные имена доменов будут включены в сертификат точки распространения. Если имена доменов, используемые мобильными устройствами, не совпадают с общим именем в сертификате точки распространения, мобильные устройства не подключаются к точке распространения.

    Имя DNS-домена по умолчанию – это полное имя домена шлюза соединения.

В обоих случаях сертификаты проверяются во время установки TLS-сеанса только на точке распространения. Сертификаты не пересылаются на проверку Сервером администрирования. После установки TLS-сеанса с мобильным устройством точка распространения использует сертификат Сервера администрирования для создания туннеля для синхронизации между мобильным устройством и Сервером администрирования. Если вы откроете порт для двусторонней SSL-аутентификации, единственный способ распространить сертификат мобильного устройства – это с помощью установочного пакета.

- Настройте опрос доменов Windows, Active Directory и IP-диапазонов точкой распространения:

  - **Windows-домены**

    Вы можете включить обнаружение устройств для Windows-доменов и задать его расписание.

  - **Контроллеры 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.

Если вы выбрали параметр **Включить опрос контроллеров домена**, вы можете выбрать контроллеры домена для опроса и задать расписание.

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.

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**

- **IP-диапазоны;**

  Вы можете включить обнаружение устройств для IPv4-диапазонов и IPv6-сетей.

  Если вы включили параметр **Разрешить опрос диапазона**, вы можете добавить диапазон опроса и задать расписание опроса. Вы можете добавить IP-диапазоны в список опрашиваемых диапазонов.

  Если включить параметр **Использовать Zeroconf для опроса IPv6-сетей**, точка распространения выполняет опрос IPv6-сети, используя сеть с нулевой конфигурацией (далее также *Zeroconf*). В этом случае указанные IP-диапазоны игнорируются, так как точка распространения опрашивает всю сеть. Параметр **Использовать Zeroconf для опроса IPv6-сетей** доступен, если точка распространения работает под управлением Linux. Чтобы использовать опрос Zeroconf IPv6, вам нужно установить утилиту avahi-browse на точке распространения.

- В разделе **Дополнительно** укажите папку, которую точка распространения должна использовать для хранения распространяемых данных:

  - **Использовать папку по умолчанию**

    При выборе этого варианта для сохранения данных будет использоваться папка, в которую на точке распространения установлен Агент администрирования.

  - **Использовать указанную папку**

    При выборе этого варианта в расположенном ниже поле можно указать путь к папке. Папка может размещаться как локально на точке распространения, так и удаленно, на любом из устройств, входящих в состав сети организации.

    Учетная запись, под которой на точке распространения запускается Агент администрирования, должна иметь доступ к указанной папке для чтения и записи.

10. Нажмите на кнопку **OK**.

В результате выбранные устройства будут выполнять роль точек распространения.

Изменение списка точек распространения для группы администрирования

Вы можете просмотреть список точек распространения, назначенных для определенной группы администрирования, и изменить список, добавив или удалив точки распространения.

Чтобы просмотреть и изменить список точек распространения для группы администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. В поле **Текущий путь** над списком управляемых устройств перейдите по ссылке.
3. В открывшейся панели слева выберите группу администрирования, для которой вы хотите просмотреть назначенные точки распространения.

   Для этого используйте пункт меню **Точки распространения**.
4. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Точки распространения**.
5. Чтобы добавить точки распространения для группы администрирования, нажмите на кнопку **Назначить** над списком управляемых устройств и выберите устройства в открывшейся панели.
6. Чтобы удалить назначенные точки распространения, выберите устройства из списка и нажмите на кнопку **Отменить назначение**.

В зависимости от изменений, точки распространения добавляются в список или существующие точки распространения удаляются из списка.

Принудительная синхронизация

Kaspersky Security Center автоматически синхронизирует состояние, параметры, задачи и политики для управляемых устройств, но в некоторых случаях вам может потребоваться запустить синхронизацию для указанного устройства принудительно. Вы можете запустить принудительную синхронизацию для следующих устройств:

- Устройств с установленным Агентом администрирования.
- Устройств под управлением KasperskyOS.

  Перед запуском принудительной синхронизации для устройства под управлением KasperskyOS убедитесь, что устройство включено в область действия точки распространения и что на точке распространения включен push-сервер.
- iOS-устройств.
- Android-устройств.

  Перед запуском принудительной синхронизации для Android-устройства необходимо настроить Firebase Cloud Messaging.

Синхронизация одного устройства

Чтобы осуществить принудительную синхронизацию между Сервером администрирования и управляемым устройством:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. Выберите имя устройства, которое требуется синхронизировать с Сервером администрирования.

   В открывшемся окне свойств выберите раздел **Общие**.
3. Нажмите на кнопку **Синхронизировать принудительно**.

Приложение выполняет синхронизацию выбранного устройства с Сервером администрирования.

Синхронизация нескольких устройств

Чтобы осуществить принудительную синхронизацию между Сервером администрирования и несколькими управляемыми устройствами:

1. Откройте список устройств группы администрирования или выборку устройств:
   - В главном меню перейдите в раздел **Активы (Устройства)**→ **Управляемые устройства**, перейдите по ссылке в поле **Текущий путь** над списком управляемых устройств и выберите группу администрирования, в которую входят устройства для синхронизации.
   - Запустите выборку устройств, чтобы просмотреть список устройств.
2. Установите флажки рядом с устройствами, которые требуется синхронизировать с Сервером администрирования.
3. Над списком управляемых устройств нажмите на кнопку с многоточием (...), а затем нажмите на кнопку **Синхронизировать принудительно**.

   Приложение выполняет синхронизацию выбранных устройств с Сервером администрирования.
4. В списке устройств проверьте, что время последнего подключения к Серверу администрирования для выбранных устройств изменилось на текущее время. Если время не изменилось, обновите содержимое страницы, нажав на кнопку **Обновить**.

Выбранные устройства синхронизированы с Сервером администрирования.

Просмотр времени доставки политики

После изменения политики для приложения "Лаборатории Касперского" на Сервере администрирования администратор может проверить, доставлена ли измененная политика на определенные управляемые устройства. Политика может быть доставлена во время регулярной или принудительной синхронизации.

Чтобы просмотреть дату и время доставки политики приложения на управляемые устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. Выберите имя устройства, которое требуется синхронизировать с Сервером администрирования.

   В открывшемся окне свойств выберите раздел **Общие**.
3. Выберите вкладку **Приложения**.
4. Выберите приложение, для которого требуется посмотреть дату синхронизации политики.

   Откроется окно политики приложения, с выбранным разделом **Общие**, и отобразится дата и время доставки политики.

Включение push-сервера

В Kaspersky Security Center точка распространения может работать как push-сервер для устройств, которые управляются по мобильному протоколу, и для устройств под управлением Агента администрирования. Например, push-сервер должен быть включен, если вы хотите включить принудительную синхронизацию устройств с KasperskyOS с Сервером администрирования. Push-сервер имеет ту же область управляемых устройств, что и точка распространения, на которой включен push-сервер. Если у вас есть несколько точек распространения, назначенных для одной и той же группы администрирования, вы можете включить извещающий сервер на каждой них. В этом случае Сервер администрирования распределяет нагрузку между точками распространения.

Возможно, вы захотите использовать точки распространения в качестве push-серверов, чтобы обеспечить постоянную связь между управляемым устройством и Сервером администрирования. Постоянное соединение необходимо для некоторых операций, таких как запуск и остановка локальных задач, получение статистики для управляемого приложения или создание туннеля. Если вы используете точку распространения в качестве push-сервера, вам не нужно использовать параметр **Не разрывать соединение с Сервером администрирования** на управляемых устройствах или отправлять пакеты на UDP-порт Агента администрирования.

Push-сервер поддерживает нагрузку до 50 000 одновременных подключений.

Чтобы включить push-сервер на точке распространения:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На вкладке **Общие** выберите раздел **Точки распространения**.
3. Нажмите на имя точки распространения, на которой вы хотите включить push-сервер.

   Откроется окно свойств точки распространения.
4. В разделе **Общие** включите параметр **Запустить push-сервер**.
5. В поле **Порт push-сервера** укажите номер порта. Вы можете указать номер любого свободного порта.

6. В поле **Адрес удаленного устройства** укажите IP-адрес или имя точки распространения.

7. Нажмите на кнопку **ОК**.

Push-сервер включен на выбранной точке распространения.

Управление приложениями сторонних производителей на клиентских устройствах

В этом разделе описаны возможности Kaspersky Security Center, связанные с управление сторонних приложений, установленных на клиентских устройствах.

Установка обновлений приложений сторонних производителей

Kaspersky Security Center позволяет управлять обновлениями программного обеспечения сторонних производителей, установленного на управляемых устройствах, и закрывать уязвимости в приложениях Microsoft и других производителей программного обеспечения с помощью установки необходимых обновлений.

Kaspersky Security Center выполняет поиск обновлений с помощью задачи *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Сервер администрирования получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, указанных в свойствах задачи и установленных на устройствах. После просмотра информации о доступных обновлениях вы можете выполнить установку обновлений на устройства.

> Обновление некоторых приложений Kaspersky Security Center выполняет путем удаления предыдущей версии приложения и установки новой версии.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Из соображений безопасности любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных приложений с помощью технологий "Лаборатории Касперского". Эти технологии используются для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение.

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 закрытия уязвимостей*.

  Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для установки обновлений для приложений Microsoft, включая обновления, предоставляемые службой Центра обновления Windows, и обновления приложений других поставщиков. Обратите внимание, что эту задачу можно создать, только если у вас есть лицензия на Системное администрирование.

  После завершения работы этой задачи обновления устанавливаются на управляемые устройства автоматически. При загрузке метаданных новых обновлений в хранилище Сервера администрирования Kaspersky Security Center проверяет, соответствуют ли обновления критериям, указанным в правилах обновлений. Все новые обновления, которые соответствуют критериям, будут загружены и установлены автоматически при следующем запуске задачи.

- Задача *Установка обновлений Центра обновления Windows*.

  Задача *Установка обновлений Центра обновления Windows* не требует лицензии, но ее можно использовать только для установки обновлений Центра обновления Windows.

  После завершения работы этой задачи устанавливаются только те обновления, которые указаны в свойствах задачи. Позже, если вы захотите установить новые обновления, загруженные в хранилище Сервера администрирования, вам будет необходимо добавить требуемые обновления в список обновлений существующей задачи или создать задачу Установка обновлений Центра обновления Windows.

Использовать Сервер администрирования в роли WSUS-сервера

Информация о доступных обновлениях Microsoft Windows передается из центра обновлений Windows. Сервер администрирования может использоваться в роли сервера Windows Update (WSUS). Чтобы использовать Сервер администрирования в качестве WSUS-сервера, вам нужно создать задачу Синхронизация обновлений Windows Update и выберите параметр **Использовать Сервер администрирования в роли WSUS-сервера** в политике Агента администрирования. После настройки синхронизации данных с центром обновлений Windows Сервер администрирования с заданной периодичностью централизованно предоставляет обновления службам Windows Update на устройствах.

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.

Предварительные требования

Сервер администрирования должен иметь подключение к интернету для установки обновлений приложений сторонних производителей, отличных от приложений Microsoft.

По умолчанию Сервер администрирования не требует подключения к интернету для установки обновлений приложений Microsoft на управляемые устройства. Например, управляемые устройства могут загружать обновления приложений Microsoft непосредственно с серверов обновлений Microsoft или с Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации. Если вы используете Сервер администрирования в качестве сервера WSUS, Сервер администрирования должен быть подключен к интернету.

Этапы

Обновление производителей состоит из следующих этапов:

1. **Поиск требуемых обновлений**

   Чтобы найти обновления приложений сторонних производителей, необходимые для управляемых устройств, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Kaspersky Security Center получает списки обнаруженных уязвимостей и требуемых обновлений для 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:

   - Консоль администрирования: Поиск уязвимостей в приложениях, Задание расписания для задачи поиска уязвимостей и требуемых обновлений.
   - Kaspersky Security Center Web Console: Создание задачи Поиск уязвимостей и требуемых обновлений, Параметры задачи поиска уязвимостей и требуемых обновлений.

2. **Анализ списка найденных обновлений**

   Просмотрите список **Обновления программного обеспечения** 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 клиентских устройствах.

   Инструкции:

   - Консоль администрирования: Просмотр информации о доступных обновлениях.
   - Kaspersky Security Center Web Console: Просмотр информации о доступных обновлениях приложений сторонних производителей.

3. **Настройка установки обновлений**

   После того как Kaspersky Security Center получает список обновлений приложений сторонних производителей, вы можете установить их на клиентские устройства, используя задачу *Установка требуемых обновлений и закрытия 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 программного обеспечения**.

   Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для установки обновлений для приложений Microsoft, включая обновления, предоставляемые службой Центра обновления Windows, и обновления приложений других поставщиков. Обратите внимание, что эту задачу можно создать, только если у вас есть лицензия на Системное администрирование.

   Задача *Установка обновлений Центра обновления Windows* не требует лицензии, но ее можно использовать только для установки обновлений Центра обновления Windows.

Для установки некоторых обновлений программного обеспечения вам нужно принять Лицензионное соглашение для установки программного обеспечения. Если вы отклоните Лицензионное соглашение, обновления программного обеспечения не будут установлены.

Вы можете запустить задачу установки обновления по расписанию. При указании расписания задачи убедитесь, что задача установки обновления запускается после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

Инструкции:

- Консоль администрирования: Закрытие уязвимостей в приложениях, Просмотр информации о доступных обновлениях.
- Kaspersky Security Center Web Console: 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, задача *Поиск уязвимостей и требуемых обновлений* настроена на запуск вручную.

Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете задать ее запуск с той же периодичностью или реже, что и запуск задачи *Поиск уязвимостей и требуемых обновлений*. 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 установки обновлений запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

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.

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.

По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус на *Одобрено* или *Отклонено* в списке **Обновления программного обеспечения** (**Операции** → **Управление патчами** → **Обновления программного обеспечения**).

Инструкции:

- Консоль администрирования: Одобрение и отклонение обновлений программного обеспечения.
- Kaspersky Security Center Web Console: Одобрение и отклонение обновлений приложений сторонних производителей.

6. **Настройка Сервера администрирования для работы в качестве службы Windows Server Update Services (WSUS) (если требуется)**

   По умолчанию обновления Центра обновления Windows загружаются на управляемые устройства с серверов Microsoft. Вы можете изменить этот параметр, чтобы использовать Сервер администрирования в роли WSUS-сервера. В этом случае Сервер администрирования синхронизирует данные обновления с Центром обновления Windows с заданной периодичностью и предоставляет обновления централизовано службам Центра обновления Windows на сетевых устройствах.

   Чтобы использовать Сервер администрирования в качестве сервера WSUS, создайте задачу Синхронизация обновлений Windows Update и установите флажок **Использовать Сервер администрирования в роли WSUS-сервера** в политике Агента администрирования.

   Инструкции:

   - Консоль администрирования: Синхронизация обновлений Windows Update с Сервером администрирования, Настройка обновлений Windows в политике Агента администрирования.
   - Kaspersky Security Center Web Console: Создание задачи Синхронизация обновлений Windows Update.

7. **Запуск задачи установки обновлений**

   Запустите задачу *Установка требуемых обновлений и закрытия 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*.

8. **Создание отчета о результатах установки обновлений приложений сторонних производителей (если требуется)**

   Чтобы просмотреть статистику установки обновления, сформируйте **Отчет о результатах установки обновлений стороннего ПО**.

   Инструкции:

   - Консоль администрирования: Создание и просмотр отчета.
   - Kaspersky Security Center Web Console: Генерация и просмотр отчета.

Результаты

Если вы создали и настроили задачу *Установка требуемых обновлений и закрытия уязвимостей*, обновления будут автоматически установлены на управляемые устройства. При загрузке новых обновлений в хранилище Сервера администрирования Kaspersky Security Center проверяет, соответствуют ли они критериям, указанным в правилах обновлений. Все новые обновления, которые соответствуют критериям, будут установлены автоматически при следующем запуске задачи.

Если вы создали задачу *Установка обновлений Центра обновления Windows*, будут установлены только те обновления, которые указаны в свойствах задачи *Установка обновлений Центра обновления Windows*. Позже, если вы захотите установить новые обновления, загруженные в хранилище Сервера администрирования, вам будет необходимо добавить требуемые обновления в список обновлений существующей задачи или создать задачу *Установка обновлений Центра обновления Windows*.

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*

  Задачу *Установка требуемых обновлений и закрытие уязвимостей* можно создать, только если у вас есть лицензия на Системное администрирование. Эту задачу можно использовать для установки обновлений Центра обновления Windows, предоставленных Microsoft, и обновлений приложений других поставщиков.

- *Установка обновлений Центра обновления Windows*

  Задачу *Установка обновлений Центра обновления Windows* можно использовать только для установки только обновлений Центра обновления Windows.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Также вы можете создать задачу для установки необходимых обновлений следующими способами:

- Открыть список обновлений и указать, какие обновления устанавливать.

  В результате создается задача для установки выбранных обновлений. Также вы можете добавить выбранные обновления в существующую задачу.

- Запустить мастер установки обновлений.

  Мастер установки обновления доступен при наличии лицензии на Системное администрирование.

  Мастер упрощает создание и настройку задачи установки обновлений и позволяет исключить создание избыточных задач, содержащих те же самые обновления для установки.

Установка обновлений приложений сторонних производителей с помощью списка обновлений

Чтобы установить обновления приложений сторонних производителей:

1. Откройте один из списков обновлений:

   - Чтобы открыть список общих обновлений, в главном меню перейдите в раздел **Операции** → **Управление патчами** → **Обновления программного обеспечения**.

   - Чтобы открыть список обновлений для управляемого устройства, в главном меню перейдите в раздел **Активы (Устройства)** → **Управляемые устройства** → <имя устройства> → **Дополнительно** → **Применимые обновления**.

   - Чтобы открыть список обновлений для определенного приложения, в главном меню перейдите в раздел **Операции** → **Приложения сторонних производителей** → **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 установятся.

4. Выберите один из следующих вариантов:

   - **Новая задача**

     Запустится мастер создания задачи. Если у вас есть лицензия на Системное администрирование, по умолчанию выбирается тип задачи *Установка требуемых обновлений и закрытие уязвимостей*. Если у вас нет лицензии, по умолчанию выбирается тип задачи *Установка обновлений Центра обновления Windows*. Следуйте далее указаниям мастера, чтобы завершить создание задачи.

   - **Установить обновление (добавить правило в указанную задачу)**

     Выберите задачу, в которую вы хотите добавить выбранные обновления. Если у вас есть лицензия на Системное администрирование, выберите задачу *Установка требуемых обновлений и закрытие уязвимостей*. Новое правило для установки выбранных обновлений будет автоматически добавлено в выбранную задачу. Если у вас нет лицензии, по умолчанию выбран тип задачи *Установка обновлений Центра обновления Windows*. Выбранные обновления добавлены в свойства задачи.

     Откроется окно свойств задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы выбрали создание задачи, она создается и отображается в списке задач в разделе **Активы (Устройства)** → **Задачи**. Если вы выбрали добавление обновлений в существующую задачу, обновления сохраняются в свойствах задачи.

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

Мастер установки обновления доступен при наличии лицензии на Системное администрирование.

Чтобы создать задачу установки обновлений приложений сторонних производителей с помощью мастера установки обновления:

1. В главном меню перейдите в раздел **Операции** → **Управление патчами** → **Обновления программного обеспечения**.

   Отобразится список доступных обновлений.

2. Установите флажок рядом с обновлением, которое вы хотите установить.

3. Нажмите на кнопку **Запустить мастер установки обновления**.

Запустится мастер установки обновления. На странице **Выбор задачи установки обновления** отображается список всех существующих задач следующих типов:

- *Установка требуемых обновлений и 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**

       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**

  Этот параметр доступен только для обновлений приложений сторонних производителей. Kaspersky Security Center 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**

  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**

  Этот параметр доступен только для обновлений приложений сторонних производителей. Kaspersky Security Center 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 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 **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Security Center выберите тип задачи **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 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 (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 не запрашивает информацию об обновлениях.

- **Поиск уязвимостей и обновлений сторонних производителей, перечисленных "Лабораторией Касперского"**

  Если этот параметр включен, Kaspersky Security Center выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите пути для дополнительного поиска приложений в файловой системе**. Полный список поддерживаемых приложений сторонних производителей контролируется "Лабораторией Касперского".

  Если этот параметр выключен, Kaspersky Security Center не выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних приложений.

  По умолчанию параметр включен.

- **Укажите пути для дополнительного поиска приложений в файловой системе**

  Папки, в которых Kaspersky Security Center выполняет поиск сторонних приложений, требующих закрытия уязвимостей и установки обновлений. Вы можете использовать системные переменные.

  Укажите папки, в которые были установлены приложения. По умолчанию список содержит системные папки, в которые устанавливается большинство приложений.

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать файлы трассировки, даже если запись файлов трассировки выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

  При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

  По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

  По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

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 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 (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 не запрашивает информацию об обновлениях.

- **Поиск уязвимостей и обновлений сторонних производителей, перечисленных "Лабораторией Касперского"**

  Если этот параметр включен, Kaspersky Security Center выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите пути для дополнительного поиска приложений в файловой системе**. Полный список поддерживаемых приложений сторонних производителей контролируется "Лабораторией Касперского".

  Если этот параметр выключен, Kaspersky Security Center не выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних приложений.

  По умолчанию параметр включен.

- **Укажите пути для дополнительного поиска приложений в файловой системе**

  Папки, в которых Kaspersky Security Center выполняет поиск сторонних приложений, требующих закрытия уязвимостей и установки обновлений. Вы можете использовать системные переменные.

  Укажите папки, в которые были установлены приложения. По умолчанию список содержит системные папки, в которые устанавливается большинство приложений.

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать файлы трассировки, даже если запись файлов трассировки выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

  При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

  По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

  По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

Рекомендации по настройке расписания запуска задачи

При планировании расписания запуска задачи *Поиск уязвимостей и требуемых обновлений* убедитесь, что включены два параметра **Запускать пропущенные задачи** и **Использовать автоматическое определение случайного интервала между запусками задачи**.

По умолчанию задача *Поиск уязвимостей и требуемых обновлений* 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

Задача *Установка требуемых обновлений и закрытие уязвимостей* доступна при наличии лицензии на Системное администрирование.

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для обновления и закрытия уязвимостей в приложениях сторонних производителей, 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*.

Чтобы создать задачу Установка требуемых обновлений и закрытие уязвимостей:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Security Center выберите тип задачи **Установка требуемых обновлений и закрытие уязвимостей**.

   Если задача не отображается, проверьте, есть ли у вашей учетной записи права **Чтение**, **Изменение** и **Выполнение** в функциональной области **Управление системой**: **Системное администрирование**. Вы не можете создавать и настраивать задачу *Установка требуемых обновлений и закрытие уязвимостей* без этих прав доступа.
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.

- **Загружать обновления на устройство, не устанавливая их**

  Если флажок установлен, приложение загружает обновления на устройство, но не устанавливает их автоматически. Затем вы можете вручную установить загруженные обновления.

  Обновления Microsoft загружаются в служебную папку Windows. Обновления сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) загружаются в папку, указанную в поле **Загрузить обновления для**.

  Если этот параметр выключен, обновления автоматически устанавливаются на устройство.

  По умолчанию параметр выключен.

- **Загрузить обновления для**

  Эта папка используется для загрузки обновлений сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft).

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать файлы трассировки, даже если запись файлов трассировки выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

  При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

  По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

  По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

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 сессиях через (мин)**

  Принудительное завершение работы приложений, когда устройство пользователя заблокировано (автоматически после периода неактивности или вручную).

  Если параметр включен, работа приложений на заблокированном устройстве принудительно прекращается по истечении времени, указанного в поле ввода.

  Если параметр выключен, работа приложений на заблокированном устройстве не прекращается.

  По умолчанию параметр выключен.

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.

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

Эта функциональность доступна при наличии лицензии на Системное администрирование.

При установке обновлений программного обеспечения или закрытии уязвимостей в приложениях с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей* необходимо указать правила установки обновлений. Эти правила определяют обновления для установки и уязвимости к закрытию.

Точные параметры зависят от того, добавляете ли вы правило для всех обновлений Центра обновления Windows или для обновлений приложений сторонних производителей (то есть приложений производства не "Лаборатории Касперского" и не Microsoft). При добавлении правила для 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 управляемые устройства.

Если у вас нет лицензии на Системное администрирование, вы не можете создавать задачи с типом *Установка обновлений Центра обновления Windows*. Чтобы установить новые обновления, вы можете добавить их в существующую задачу *Установка обновлений Центра обновления Windows*. Рекомендуется использовать задачу *Установка требуемых обновлений и закрытие уязвимостей* вместо задачи *Установка обновлений Центра обновления Windows*. Задача *Установка требуемых обновлений и закрытие уязвимостей* позволяет автоматически устанавливать несколько обновлений и закрывать несколько уязвимостей в соответствии с заданными правилами. Также эта задача позволяет устанавливать обновления для приложений сторонних производителей, то есть приложений производства не Microsoft.

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 Установка обновлений Центра обновления Windows:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для приложения Kaspersky Security Center выберите тип задачи **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 программного обеспечения**.

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 **Активы (Устройства)** → **Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием устройства, для которого вы хотите просмотреть обновления приложений сторонних производителей.

   Откроется окно свойств выбранного устройства.

3. В окне свойств выбранного устройства выберите вкладку **Дополнительно**.

4. На левой панели выберите раздел **Применимые обновления**. Если вы хотите просматривать только установленные обновления, включите параметр **Показывать установленные обновления**.

Отобразится список доступных обновлений приложений сторонних производителей для выбранного устройства.

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 программного обеспечения**.

   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 программного обеспечения**.

   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 программного обеспечения**.

   Отобразится список доступных обновлений.

2. Выберите обновление, которое требуется одобрить или отклонить.

   Откроется окно свойств обновления.

3. В разделе **Общие** выберите статус обновления, 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.

Создание задачи Синхронизация обновлений Windows Update

Задача *Синхронизация обновлений Windows Update* доступна при наличии лицензии на Системное администрирование.

Задача *Синхронизация обновлений Windows Update* требуется, если вы хотите использовать Сервер администрирования в роли WSUS-сервера. В этом случае Сервер администрирования загружает обновления Windows в базу данных и предоставляет обновления Центра обновления Windows на клиентских устройствах в централизованном режиме с помощью Агентов администрирования. Если в сети не используется WSUS-сервер, то каждое клиентское устройство самостоятельно загружает обновления Microsoft с внешних серверов.

Задача *Синхронизация обновлений Windows Update* загружает с серверов Microsoft только метаданные. Во время выполнения задачи установки обновлений, Kaspersky Security Center загружает только те обновления, которые вы выбрали для установки.

Во время выполнения задачи **Синхронизация обновлений Windows Update**, приложение получает список актуальных обновлений с сервера обновлений Microsoft. После чего Kaspersky Security Center определяет список устаревших обновлений. При следующем запуске задачи **Поиск уязвимостей и требуемых обновлений** Kaspersky Security Center отмечает устаревшие обновления и устанавливает время на удаление. При следующем запуске задачи **Синхронизация обновлений Windows Update** удаляются обновления, которые были отмечены на удаление 30 дней назад. Kaspersky Security Center также выполняет дополнительную проверку для удаления устаревших обновлений, которые были отмечены на удаление более 180 дней назад.

После завершения работы задачи **Синхронизация обновлений Windows Update** и удаления устаревших обновлений в базе данных могут оставаться хеш-коды файлов удаленных обновлений, а также соответствующие им файлы в папке %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles, в случае если они были загружены ранее. С помощью задачи **Обслуживание Сервера администрирования** можно удалить такие устаревшие записи из базы данных и соответствующие им файлы.

Чтобы создать задачу Синхронизация обновлений Windows Update:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

3. Для приложения Kaspersky Security Center выберите тип задачи **Синхронизация обновлений Windows Update**.

4. Укажите название задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

5. Включите параметр **Загрузить файлы экспресс-установки**, если вы хотите, чтобы файлы экспресс-обновления загружались при выполнении задачи.

   Когда Kaspersky Security Center синхронизирует обновления с серверами Microsoft Windows Update Servers, информация обо всех файлах сохраняется в базе данных Сервера администрирования. Также на диск загружаются все файлы, необходимые для обновления, при взаимодействии с Агентом обновления Windows. В частности, Kaspersky Security Center сохраняет информацию о файлах экспресс-установки в базу данных и загружает их по мере необходимости. Загрузка файлов экспресс-установки приводит к сокращению свободного места на диске.

   Чтобы уменьшить сокращение объема дискового пространства и снизить трафик, выключите параметр **Загрузить файлы экспресс-установки**.

6. Выберите приложения, для которых требуется загрузить обновления.

   Если установлен флажок **Все приложения**, то обновления будут загружаться для всех имеющихся приложений, а также для тех приложений, которые могут быть выпущены в будущем.

7. Выберите категории обновлений, которые вы хотите загрузить на Сервер администрирования.

   Если установлен флажок **Все категории**, то обновления будут загружаться для всех имеющихся категорий обновлений, а также для тех категорий, которые могут появиться в будущем.

8. Выберите языки локализации обновлений, которые вы хотите загрузить на Сервер администрирования. Выберите один из следующих вариантов:

   - **Загружать все языки, включая новые**

     Если выбран этот вариант, на Сервер администрирования будут загружаться все доступные языки локализации обновлений. По умолчанию выбран этот вариант.

   - **Загружать выбранные языки**

     Если выбран этот вариант, в списке можно выбрать языки локализации обновлений, которые должны загружаться на Сервер администрирования.

9. Укажите, под какой учетной записью запускать задачу. Выберите один из следующих вариантов:

   - **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.

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.

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 → Приложения сторонних производителей → Реестр приложений**.

2. Нажмите на имя приложения, для которого вы хотите изменить параметр автоматического обновления.

   Чтобы упростить поиск, вы можете отфильтровать список по 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 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 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.

Закрытие уязвимостей в приложениях сторонних производителей

В этом разделе описаны возможности Kaspersky Security Center связанные с закрытием уязвимостей в приложениях, установленных на управляемых устройствах.

Сценарий: обнаружение и закрытие уязвимостей в приложениях сторонних производителей

В этом разделе представлен сценарий обнаружения и закрытия уязвимостей на управляемых устройствах под управлением Windows. Вы можете обнаружить и закрыть уязвимости в операционной системе и в стороннем программном обеспечении, включая программное обеспечение Microsoft.

Предварительные требования

- Kaspersky Security Center развернут в вашей организации.
- В сети вашей организации есть управляемые устройства под управлением Windows.
- Подключение Сервера администрирования к интернету необходимо для выполнения следующих задач:
  - Составление списка рекомендуемых исправлений уязвимостей в приложениях Microsoft. Список формируется и регулярно обновляется специалистами "Лаборатории Касперского".
  - Закрытие уязвимостей в приложениях сторонних производителей, отличных от приложений Microsoft.

Этапы

Обнаружение и закрытие уязвимостей состоит из следующих этапов:

1. **Поиск уязвимостей в программном обеспечении, установленном на управляемых устройствах**

Чтобы найти уязвимости в приложениях, установленных на управляемых устройствах, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Kaspersky Security Center получает 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. Если вы не запускали мастер первоначальной настройки, запустите его сейчас или создайте задачу вручную.

Инструкции:

- Консоль администрирования: Поиск уязвимостей в приложениях, Задание расписания для задачи поиска уязвимостей и требуемых обновлений.
- Kaspersky Security Center Web Console: Создание задачи Поиск уязвимостей и требуемых обновлений, Параметры задачи поиска 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:

- Консоль администрирования: Просмотр информации об уязвимостях в приложениях, Просмотр статистики уязвимостей на управляемых устройствах.
- Kaspersky Security Center Web Console: 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. Обратите внимание, что эту задачу можно создать, только если у вас есть лицензия на Системное администрирование. Чтобы устранить уязвимости в приложениях, задача *Установка требуемых обновлений и закрытие уязвимостей* использует рекомендованные обновления приложений.

Задача *Закрытие уязвимостей* не требует лицензии для Системного администрирования. Чтобы использовать эту задачу, требуется вручную указать пользовательские исправления для закрытия уязвимостей в приложениях сторонних производителей, которые указаны в параметрах задачи. Задача *Закрытие уязвимостей* использует рекомендованные исправления приложений Microsoft и пользовательские исправления для приложений сторонних производителей.

Вы можете запустить мастер закрытия уязвимостей, который автоматически создаст одну из этих задач, или вы можете создать одну из этих задач вручную.

Инструкции:

- Консоль администрирования: Пользовательские исправления для уязвимостей в приложениях сторонних производителей, Закрытие уязвимостей в приложениях.
- Kaspersky Security Center Web Console: Пользовательские исправления для уязвимостей в приложениях сторонних производителей, 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 или реже, что и запуск задачи *Поиск уязвимостей и требуемых обновлений*. При задании расписания задачи *Закрытие уязвимостей*, вам нужно выбрать исправления приложений Microsoft или указать пользовательские исправления для приложений сторонних производителей каждый раз перед запуском задачи.

   При задании расписания задач убедитесь, что задача закрытия уязвимостей запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

5. **Игнорирование уязвимостей в приложениях (если требуется)**

   Вы можете игнорировать уязвимости в приложениях, которые должны быть закрыты на всех управляемых устройствах или только на выбранных управляемых устройствах.

   Инструкции:

   - Консоль администрирования: Игнорирование уязвимостей в приложениях.
   - Kaspersky Security Center Web Console: Игнорирование уязвимостей в приложениях.

6. **Запуск задачи закрытия уязвимости**

   Запустите задачу *Установка требуемых обновлений и закрытия уязвимостей* или *Закрытие уязвимостей*. Когда задача будет завершена, убедитесь, что в списке задач она имеет статус *Завершена успешно*.

7. **Создание отчета о результатах закрытия уязвимостей в приложениях (если требуется)**

   Чтобы просмотреть статистику о закрытых уязвимостях, сформируйте отчет об уязвимостях. 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.

   Инструкции:

   - Консоль администрирования: Создание и просмотр отчета.
   - Kaspersky Security Center Web Console: Генерация и просмотр отчета.

8. **Проверка настройки обнаружения и закрытия уязвимостей в приложениях сторонних производителей**

   Убедитесь, что вы выполнили следующее:

   - обнаружили и просмотрели список уязвимостей в приложениях на управляемых устройствах;
   - игнорировали уязвимости в приложениях, если хотели;
   - настроили задачу закрытия уязвимости;
   - запланировали запуск задач для поиска и закрытия уязвимостей в приложениях так, чтобы они запускались последовательно;
   - проверили, что задача закрытия уязвимостей была запущена.

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 в правилах, будут загружены в хранилище Сервера администрирования и будут установлены для закрытия уязвимостей в приложениях.

Если вы создали задачу *Закрытие уязвимостей*, закрываются только уязвимости в приложениях Microsoft.

Об обнаружении и закрытии уязвимостей в приложениях

Kaspersky Security Center 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 выполняет поиск известных уязвимостей в приложениях на основе признаков из баз данных об известных уязвимостях. Эта база формируются 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 для поиска уязвимостей в приложениях используется задача *Поиск уязвимостей и требуемых обновлений*.

В некоторых случаях обнаруженные уязвимости в операционной системе Microsoft Windows можно закрыть одним из следующих способов:

- Установить обновления для операционной системы.
- Обновить операционную систему до новой версии (например, с Windows 10 до Windows 11).

В этом сценарии Kaspersky Security Center отображает две записи для одной и той же уязвимости.

Закрытие уязвимостей в приложениях

Для закрытия уязвимостей в приложениях, Kaspersky Security Center использует обновления программного обеспечения выпущенные поставщиками программного обеспечения. Метаданные обновлений программного обеспечения загружаются в хранилище Сервера администрирования в результате выполнения следующих задач:

- *Загрузка обновлений в хранилище Сервера администрирования*. Эта задача предназначена для загрузки метаданных обновлений для приложений "Лаборатории Касперского" и приложений сторонних производителей. Эта задача автоматически создается в мастере первоначальной настройки Kaspersky Security Center. Задача загрузки обновлений в хранилище Сервера администрирования может быть создана вручную.

- *Синхронизация обновлений Windows Update*. Эта задача предназначена для загрузки метаданных обновлений программного обеспечения Microsoft.

Обновления программного обеспечения для закрытия уязвимостей могут быть представлены в виде полных дистрибутивов или патчей. Обновления программного обеспечения, которые закрывают уязвимости в приложениях, называются *исправлениями*. *Рекомендуемые исправления* это исправления, которые рекомендуются к установке специалистами "Лаборатории Касперского". *Пользовательские исправления* это исправления, которые вручную указываются для установки пользователями. Чтобы установить пользовательское исправление, необходимо создать инсталляционный пакет, содержащий это исправление.

Если лицензия Kaspersky Security Center предусматривает возможности Системного администрирования, для закрытия уязвимостей используйте задачу *Установка требуемых обновлений и закрытие уязвимостей*. Эта задача автоматически закрывает несколько уязвимостей, устанавливая рекомендуемые исправления. Для этой задачи вы можете вручную настроить определенные правила для закрытия нескольких уязвимостей.

Если лицензия Kaspersky Security Center не предусматривает возможности Системного администрирования, для закрытия уязвимостей используйте задачу *Закрытие уязвимостей*. С помощью этой задачи можно закрыть уязвимости, установив рекомендуемые исправления для приложений Microsoft и пользовательских исправлений для приложений сторонних производителей.

Из соображений безопасности любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных приложений с помощью технологий "Лаборатории Касперского". Эти технологии используются для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение.

Эксперты "Лаборатории Касперского" не проводят ручной анализ обновлений приложений сторонних производителей, которые можно установить с помощью Системного администрирования. Также эксперты "Лаборатории Касперского" не занимаются поиском уязвимостей (известных или неизвестных) или недокументированных возможностей в таких обновлениях и не проводят другие виды анализа упомянутых выше обновлений.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Для закрытия некоторых уязвимостей программного обеспечения вам нужно принять Лицензионное соглашение для установки программного обеспечения, если это требуется. Если вы отклоняете Лицензионное соглашение, уязвимость в программном обеспечении не закроется.

Закрытие уязвимостей в приложениях сторонних производителей

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*.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Также вы можете создать задачу для закрытия уязвимостей в приложениях следующими способами:

- Откройте список уязвимостей и укажите, какие уязвимости необходимо закрыть.

  В результате создается задача закрытия уязвимостей в приложениях. Также можно добавить выбранные уязвимости в существующую задачу.

- Запустите мастер закрытия уязвимостей.

  Мастер закрытия уязвимости доступен при наличии лицензии на Системное администрирование.

  Мастер упрощает создание и настройку задачи закрытия уязвимостей, а также исключает создание избыточных задач, 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 **Активы (Устройства)** → **Управляемые устройства** → <имя устройства> → **Дополнительно** → **Уязвимости в приложениях**.

   - Чтобы открыть список уязвимостей для требуемого приложения, в главном меню перейдите в раздел **Операции** → **Приложения сторонних производителей** → **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 в приложениях вам нужно принять Лицензионное соглашение для установки приложений, если это требуется. Если вы отклоняете Лицензионное соглашение, уязвимость в приложении не закроется.

3. Выберите один из следующих вариантов:

   - **Новая задача**

     Запустится мастер создания задачи. Если у вас есть лицензия на Системное администрирование, по умолчанию выбирается тип задачи *Установка требуемых обновлений и закрытие уязвимостей*. Если у вас нет лицензии, по умолчанию выбирается тип задачи *Закрытие уязвимостей*. Следуйте далее указаниям мастера, чтобы завершить создание задачи.

   - **Закрыть уязвимость (добавить правило в указанную задачу)**

     Выберите задачу, в которую вы хотите добавить выбранные уязвимости. Если у вас есть лицензия на Системное администрирование, выберите задачу *Установка требуемых обновлений и закрытие уязвимостей*. В выбранную задачу будет автоматически добавлено новое правило для закрытия выбранных уязвимостей. Если у вас нет лицензии, по умолчанию выбран тип задачи *Закрытие уязвимостей*. Выбранные уязвимости 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 **Активы (Устройства)** → **Задачи**. Если вы выбрали добавление уязвимостей в существующую задачу, уязвимости сохраняются в свойствах задачи.

Чтобы закрыть уязвимости в приложениях сторонних производителей, запустите задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Закрытие уязвимостей*. Если вы создали задачу *Закрытие уязвимостей*, вам нужно вручную указать обновления программного обеспечения для закрытия уязвимостей, перечисленных в свойствах задачи.

Закрытие уязвимостей в приложениях с помощью мастера закрытия уязвимостей

> Мастер закрытия уязвимости доступен при наличии лицензии на Системное администрирование.

Чтобы закрыть уязвимости в приложениях с помощью мастера закрытия уязвимостей:

1. В главном окне приложения перейдите в раздел **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 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**.

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, задача *Установка требуемых обновлений и закрытие уязвимостей* добавлена в список задач.

Создание задачи Закрытие уязвимостей

Задача *Закрытие уязвимостей* позволяет закрыть уязвимости в приложениях на управляемых устройствах с операционными системами Windows. Вы можете закрыть уязвимости в приложениях сторонних производителей, включая приложения Microsoft.

Если у вас нет лицензии на Системное администрирование, вы не можете создавать задачи с типом *Закрытие уязвимостей*. Чтобы закрыть новые уязвимости, вы можете добавить их в существующую задачу *Закрытие уязвимостей*. Рекомендуется использовать задачу *Установка требуемых обновлений и закрытие уязвимостей* вместо задачи *Закрытие уязвимостей*. Задача *Установка требуемых обновлений и закрытие уязвимостей* позволяет автоматически устанавливать несколько обновлений и закрывать несколько уязвимостей в соответствии с заданными правилами.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Чтобы создать задачу Закрытие уязвимостей:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для приложения Kaspersky Security Center выберите тип задачи **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**.

   Для уязвимостей в приложениях Microsoft обычно существуют рекомендуемые исправления. Дополнительные действия для них не требуются. Для уязвимостей в приложениях сторонних производителей сначала необходимо указать исправление пользователя для каждой уязвимости, которую вы хотите закрыть. После этого вы сможете добавить эти уязвимости в задачу *Закрытие уязвимостей*.

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.

Создание задачи Установка требуемых обновлений и закрытие уязвимостей

Задача *Установка требуемых обновлений и закрытие уязвимостей* доступна при наличии лицензии на Системное администрирование.

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для обновления и закрытия уязвимостей в приложениях сторонних производителей, 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*.

Чтобы создать задачу Установка требуемых обновлений и закрытие уязвимостей:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Security Center выберите тип задачи **Установка требуемых обновлений и закрытие уязвимостей**.

   Если задача не отображается, проверьте, есть ли у вашей учетной записи права **Чтение**, **Изменение** и **Выполнение** в функциональной области **Управление системой**: **Системное администрирование**. Вы не можете создавать и настраивать задачу *Установка требуемых обновлений и закрытие уязвимостей* без этих прав доступа.
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.

- **Загружать обновления на устройство, не устанавливая их**

  Если флажок установлен, приложение загружает обновления на устройство, но не устанавливает их автоматически. Затем вы можете вручную установить загруженные обновления.

  Обновления Microsoft загружаются в служебную папку Windows. Обновления сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) загружаются в папку, указанную в поле **Загрузить обновления для**.

  Если этот параметр выключен, обновления автоматически устанавливаются на устройство.

  По умолчанию параметр выключен.

- **Загрузить обновления для**

  Эта папка используется для загрузки обновлений сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft).

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать файлы трассировки, даже если запись файлов трассировки выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

  При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

  По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

  По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

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 сессиях через (мин)**

  Принудительное завершение работы приложений, когда устройство пользователя заблокировано (автоматически после периода неактивности или вручную).

  Если параметр включен, работа приложений на заблокированном устройстве принудительно прекращается по истечении времени, указанного в поле ввода.

  Если параметр выключен, работа приложений на заблокированном устройстве не прекращается.

  По умолчанию параметр выключен.

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.

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

Эта функциональность доступна при наличии лицензии на Системное администрирование.

При установке обновлений программного обеспечения или закрытии уязвимостей в приложениях с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей* необходимо указать правила установки обновлений. Эти правила определяют обновления для установки и уязвимости к закрытию.

Точные параметры зависят от того, добавляете ли вы правило для всех обновлений Центра обновления Windows или для обновлений приложений сторонних производителей (то есть приложений производства не "Лаборатории Касперского" и не Microsoft). При добавлении правила для 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.

Пользовательские исправления для уязвимостей в приложениях сторонних производителей

Чтобы использовать задачу *Закрытие уязвимостей*, необходимо вручную указать обновления программного обеспечения, чтобы закрыть уязвимости в приложениях сторонних производителей, перечисленные в параметрах задачи. Задача *Закрытие уязвимостей* использует рекомендованные исправления приложений Microsoft и пользовательские исправления для других приложений сторонних производителей. *Пользовательские исправления* это обновления программного обеспечения для закрытия уязвимостей, которые администратор вручную указывает для установки.

Чтобы выбрать пользовательские исправления для уязвимостей в приложениях сторонних производителей:

1. В главном окне приложения перейдите в раздел **Операции → Управление патчами → Уязвимости в приложениях**.

   На странице отображается список уязвимостей в приложениях, обнаруженных на клиентских устройствах.

2. В списке уязвимостей в приложениях перейдите по ссылке с названием уязвимости, для которой вы хотите указать пользовательское исправление.

   Откроется окно свойств уязвимости.

3. В левой панели выберите раздел **Пользовательские и другие исправления**.

   Отобразится список пользовательских исправлений для выбранной уязвимости в приложениях.

4. Нажмите на кнопку **Добавить**.

   Отобразится список доступных инсталляционных пакетов. Список отобразившихся инсталляционных пакетов соответствует списку в папке **Операции → Хранилища → Инсталляционные пакеты**. Если вы не создали инсталляционный пакет, содержащий пользовательское исправление для закрытия выбранной уязвимости, вы можете создать пакет сейчас, запустив мастер создания инсталляционного пакета.

5. Выберите инсталляционный пакет (или пакеты), содержащий пользовательское исправление (или пользовательские исправления) для уязвимости приложениях сторонних производителей.

6. Нажмите на кнопку **Сохранить**.

Указаны инсталляционные пакеты, содержащие пользовательские исправления для уязвимости в приложениях. После запуска задачи *Закрытие уязвимостей* будет установлен инсталляционный пакет и закрыта уязвимость в приложениях.

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 **Активы (Устройства)** → **Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием устройства, для которого вы хотите просмотреть обнаруженные уязвимости в приложениях.

   Откроется окно свойств выбранного устройства.

3. В окне свойств выбранного устройства выберите вкладку **Дополнительно**.

4. На левой панели выберите раздел **Уязвимости в приложениях**.

   Отобразится список уязвимостей в приложениях, обнаруженных на выбранном управляемом устройстве.

Чтобы просмотреть свойства выбранной уязвимости в приложениях,

перейдите по ссылке с названием уязвимости в списке уязвимостей в приложениях.

Откроется окно свойств выбранной уязвимости в приложениях.

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 **Активы (Устройства) → Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с именем устройства, на котором вы хотите пропустить уязвимость в приложениях.

   Откроется окно свойств устройства.

3. В окне свойств устройства выберите раздел **Дополнительно**.

4. На левой панели выберите раздел **Уязвимости в приложениях**.

   Отобразится список уязвимостей в приложениях, обнаруженных на устройстве.

5. В списке уязвимостей в приложениях выберите уязвимость, которую вы хотите пропустить на выбранном устройстве.

   Откроется окно свойств уязвимости в приложениях.

6. В окне свойств уязвимости в приложениях на вкладке **Общие** включите параметр **Игнорировать уязвимость**.

7. Нажмите на кнопку **Сохранить**.

   Окно свойств уязвимости в приложениях закроется.

8. Закройте окно свойств устройства.

Уязвимость в приложениях пропускается на выбранном устройстве.

Пропущенные уязвимости в приложениях не будут закрыты после завершения работы задачи *Закрытие уязвимостей* и задачи *Установка требуемых обновлений и закрытие уязвимостей*. Вы можете исключить пропущенные уязвимости в приложениях из списка уязвимостей с помощью фильтра.

Управление запуском приложений на клиентских устройствах

В этом разделе описаны возможности Kaspersky Security Center 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.Также компонент доступен для Kaspersky Embedded Systems Security для Windows 3.0 и выше.

Предварительные требования

- Kaspersky Security Center развернут в вашей организации.
- Политика Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux создана и активна.
- Политика Kaspersky Embedded Systems Security для Windows или Kaspersky Embedded Systems 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.

   Инструкции:

   - Консоль администрирования: Инвентаризация исполняемых файлов.
   - Kaspersky Security Center Web Console: Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах.

2. **Создание категорий для исполняемых файлов, используемых в вашей организации**

Проанализируйте списки приложений и 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.

Инструкции:

- Консоль администрирования: Создание пополняемой вручную категории приложений, Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств, Создание категории приложений, в которую входят исполняемые файлы из указанных папок.
- Kaspersky Security Center Web Console: Создание пополняемой вручную категории приложений, Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств, Создание категории приложений, в которую входят исполняемые файлы из указанных папок.

3. **Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security**

   Настройте компонент Контроль приложений в политике Kaspersky Endpoint Security с использованием категорий, которые вы создали на предыдущем этапе.

   Инструкции:

   - Консоль администрирования: Настройка управления запуском приложений на клиентских устройствах.
   - Kaspersky Security Center Web Console: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows.

4. **Настройка компонента Контроль приложений в политике Kaspersky Embedded Systems Security**

   Настройте компонент Контроль приложений в политике Kaspersky Embedded Systems Security для Windows, используя созданные вами категории. Подробную информацию о компоненте Контроль приложений см. в справке Kaspersky Embedded Systems Security для Windows или в справке Kaspersky Embedded Systems Security для Linux.

   При использовании большого количества правил может возникнуть ошибка при загрузке политики. Вы можете увеличить максимальный размер JSON-запроса в байтах, используя следующую команду:

   ```
   klscflag -fset -pv ".core/.independent" -s KLLIM -n
   LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v <max_request_size> -t d
   ```

   Где `<max_request_size>` это максимальный размер запроса в байтах (например, `200000000`).

5. **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 или Kaspersky Embedded Systems Security не будет блокировать исполняемые файлы, запуск которых запрещен правилами Контроля приложений, а вместо этого будет отправлять уведомления об их запуске на Сервер администрирования.

   При тестировании правил Контроля приложений рекомендуется выполнить следующие действия:

   - Определите период тестирования. Период тестирования может варьироваться от нескольких дней до двух месяцев.
   - Изучите события, возникающие в результате тестирования работы компонента Контроль приложений.

   Инструкции для Kaspersky Security Center Web Console: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows. Следуйте этой инструкции и включите параметр **Тестовый режим** в процессе настройки.

6. **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 пополняемую вручную.

   Инструкции:

   - Консоль администрирования: Добавление исполняемых файлов, связанных с событием, в категорию приложений.
   - Kaspersky Security Center Web Console: Добавление исполняемых файлов, связанных с событием, в категорию приложений.

7. **Применение правил Контроля приложений в рабочем режиме**

   После проверки правил Контроля приложений и завершения настройки категорий вы можете применить правила Контроль приложений в рабочем режиме.

   Инструкции для Kaspersky Security Center Web Console: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows. Следуйте этой инструкции и выключите параметр **Тестовый режим** в процессе настройки.

8. **Проверка конфигурации Контроля приложений**

   Убедитесь, что вы выполнили следующее:

   - Создали категории для исполняемых файлов.
   - Настроили Контроль приложений с использованием категорий.
   - Применили правила Контроля приложений в рабочем режиме.

Результаты

После завершения сценария, запуск исполняемых файлов на управляемых устройствах контролируется. Пользователи могут запускать только те исполняемые файлы, которые разрешены в вашей организации, и не могут запускать исполняемые файлы, запрещенные в вашей организации.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux
- Kaspersky Security для виртуальных сред Легкий агент
- Справка Kaspersky Embedded Systems Security для Windows
- Справка Kaspersky Embedded Systems 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 Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security 11.2 для Linux и выше, для Kaspersky Security для виртуальных сред Легкий агент. Все инструкции в этом разделе описывают настройку Контроля приложений для приложения Kaspersky Endpoint Security для Windows.

Запуск исполняемых файлов, параметры которых не соответствуют ни одному из правил Контроля приложений, регулируется выбранным режимом работы компонента:

- *Список запрещенных*. Режим используется, если вы хотите разрешить запуск всех исполняемых файлов, кроме тех, которые указаны в запрещающих правилах. По умолчанию выбран этот режим.
- *Список разрешенных*. Режим используется, если вы хотите запретить запуск всех исполняемых файлов, кроме тех, которые указаны в разрешающих правилах.

Правила Контроля приложений реализованы в категориях для исполняемых файлов. В Kaspersky Security Center существует три 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.
- Категория, в которую входят исполняемые файлы из выбранных папок. Вы указываете папку, исполняемые файлы из которой автоматически попадают в категорию.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux
- Kaspersky Security для виртуальных сред Легкий агент
- Справка Kaspersky Embedded Systems Security для Windows
- Справка Kaspersky Embedded Systems Security для Linux

Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах

Вы можете получить список исполняемых файлов, хранящихся на клиентских устройствах, одним из следующих способов:

- Включив уведомление о запуске приложений в политике Kaspersky Endpoint Security.
- Создав задачу инвентаризации.

Включение уведомлений о запуске приложений в политике Kaspersky Endpoint Security

Чтобы включить уведомления о запуске приложения:

1. Откройте параметры политики Kaspersky Endpoint Security и перейдите на вкладку **Общие параметры** → **Отчеты и хранилища**.
2. В группе параметров **Передача данных на Сервер администрирования** установите флажок **О запущенных приложениях** и сохраните изменения.

   Когда пользователь пытается запустить исполняемые файлы, информация об этих файлах добавляется в список исполняемых файлов на клиентском устройстве. Kaspersky Endpoint Security отправляет эту информацию Агенту администрирования, а затем Агент администрирования отправляет ее на Сервер администрирования.

Создание задачи инвентаризации

Функция инвентаризации исполняемых файлов доступна для следующих приложений:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux версии 11.2 и выше
- Kaspersky Security для виртуальных сред 4.0 Легкий агент и выше

Вы можете снизить нагрузку на базу данных при получении информации об установленных приложениях. Для того чтобы сохранить место в базе данных, вам нужно запустить задачу инвентаризации на нескольких эталонных устройствах, на которых установлен стандартный набор приложений. Предпочтительное количество устройств равно 1–3.

> Настоятельно не рекомендуется выполнять задачу инвентаризации при использовании следующих баз данных: MySQL, PostgreSQL, SQL Server Express Edition, MariaDB (все версии).

Чтобы создать задачу инвентаризации исполняемых файлов на клиентских устройствах:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **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** 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
- Kaspersky Security для виртуальных сред Легкий агент

После выполнения задачи **Инвентаризация** формируется список исполняемых файлов, хранящихся на управляемых устройствах, и вы можете просмотреть этот список.

Во время инвентаризации могут быть обнаружены исполняемые файлы в следующих форматах (в зависимости от выбранного вами параметра в свойствах задачи инвентаризации): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR и HTML.

Просмотр списка приложений и исполняемых файлов, хранящихся на управляемых устройствах

Чтобы просмотреть список исполняемых файлов, хранящихся на клиентских устройствах,

В главном окне приложения перейдите в раздел **Операции → Приложения сторонних производителей → Исполняемые файлы**.

На странице отобразится список исполняемых файлов, хранящихся на клиентских устройствах.

При необходимости вы можете отправить исполняемый файл управляемого устройства на устройство, где открыта Kaspersky Security Center Web Console.

Чтобы отправить исполняемый файл:

1. В главном окне приложения перейдите в раздел **Операции → Приложения сторонних производителей → Исполняемые файлы**.

2. Перейдите по ссылке исполняемого файла, который вы хотите отправить.

3. В открывшемся окне перейдите в раздел **Устройства** и установите флажок рядом с управляемым устройством, с которого вы хотите отправить исполняемый файл.

   Перед отправкой исполняемого файла убедитесь, что управляемое устройство имеет прямое подключение к Серверу администрирования, установив флажок **Не разрывать соединение с Сервером администрирования**.

4. Нажмите на кнопку **Отправить**.

   Выбранный исполняемый файл будет загружен для дальнейшей отправки на устройство, на котором открыта Kaspersky Security Center Web Console.

Создание пополняемой вручную категории приложений

Вы можете указать набор критериев в качестве шаблона для исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов, соответствующих критериям, вы можете создать категорию приложений и использовать ее в настройке компонента Контроль приложений.

Чтобы создать пополняемую вручную категорию приложений:

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Категории приложений**.

   Откроется страница со списком категорий приложений.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге **Выбор способа создания категории** выберите параметр **Пополняемая вручную категория. Данные об исполняемых файлах добавляются в категорию вручную**.

4. На шаге **Условия** нажмите на кнопку **Добавить**, чтобы добавить критерий условия для включения файлов в создаваемую категорию.

5. На шаге **Критерии условия** выберите тип правила для создания категории из списка:

   - **Из KL-категории**

     Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать категорию приложений "Лаборатории Касперского". Приложения, входящие в указанную KL-категорию, будут добавлены в пользовательскую категорию приложений.

   - **Выберите сертификат из хранилища сертификатов**

     Если выбран этот вариант, можно указать сертификаты из хранилища. 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 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 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.

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.

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
- Kaspersky Security для виртуальных сред Легкий агент
- Справка Kaspersky Embedded Systems Security для Windows
- Справка Kaspersky Embedded Systems 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 получить список исполняемых файлов с устройств:

1. Убедитесь, что политика Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux создана и активна. Включите в политике компонент Контроль приложений.
2. Получение списка исполняемых файлов, хранящихся на клиентских устройствах.

Чтобы создать категорию, в которую входят исполняемые файлы с выбранных устройств:

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Категории приложений**.

   Откроется страница со списком категорий.

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 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 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.

Создание категории приложений, в которую входят исполняемые файлы из выбранных папок

Вы можете использовать исполняемые файлы выбранных папок как эталонный набор исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов из выбранных папок вы можете создать категорию приложений и использовать ее для настройки компонента Контроль приложений.

Чтобы создать категорию, в которую входят исполняемые файлы из выбранных папок:

1. В главном окне приложения перейдите в раздел **Операции → Приложения сторонних производителей → Категории приложений**.

   Откроется страница со списком категорий.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге **Выбор способа создания категории**, укажите имя категории и выберите параметр **Категория, в которую входят исполняемые файлы из указанной папки. Исполняемые файлы приложений, копируемых в указанную папку, обрабатываются автоматически, и их метрики заносятся в категорию**.

4. Укажите папку, исполняемые файлы которой будут использоваться для создания категории.

5. Настройте следующие параметры:

   - **Включать в категорию динамически подключаемые библиотеки (DLL)**

     В категорию приложений включаются динамически подключаемые библиотеки (файлы формата DLL), и компонент Контроль приложений регистрирует действия таких библиотек, запущенных в системе. При включении файлов формата DLL в категорию возможно снижение производительности работы Kaspersky Security Center.

     По умолчанию флажок снят.

   - **Включать в категорию данные о скриптах**

     В категорию приложений включаются данные о скриптах, и скрипты не блокируются компонентом Защита от веб-угроз. При включении данных о скриптах в категорию возможно снижение производительности работы Kaspersky Security Center.

     По умолчанию флажок снят.

   - **Алгоритм вычисления хеш-функции**: **Вычислять SHA256 для файлов в категории (поддерживается для версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше) / Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**

     В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky Security Center для файлов категории. Информация о 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 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.

- **Принудительно проверять папку на наличие изменений**

  Если этот параметр включен, приложение периодически принудительно проверяет папку пополнения категорий на наличие изменений. Периодичность проверки в часах можно указать в поле ввода рядом с флажком. По умолчанию период принудительной проверки равен 24 часам.

  Если этот параметр выключен, принудительная проверка папки не выполняется. Сервер обращается к файлам в папке в случае их изменения, добавления или удаления.

  По умолчанию параметр выключен.

После завершения работы мастера создается категория исполняемых файлов. Она появится в списке категорий. Вы можете использовать категорию для настройки 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
- Kaspersky Security для виртуальных сред Легкий агент
- Справка Kaspersky Embedded Systems Security для Windows
- Справка Kaspersky Embedded Systems Security для Linux

Просмотр списка категорий приложений

Вы можете просмотреть список настроенных категорий исполняемых файлов и параметры каждой категории.

Чтобы просмотреть список категорий приложений,

В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Категории приложений**.

Откроется страница со списком категорий.

Чтобы просмотреть свойства категории приложений,

нажмите на имя категории.

Откроется окно свойств выбранной категории. Параметры сгруппированы на нескольких вкладках.

Добавление исполняемых файлов, связанных с событием, в категорию приложения

После настройки компонента 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 и отчеты** → **Выборки событий**.

   Отобразится список выборок событий.

2. Выберите выборку событий, чтобы просмотреть события, связанные с Контролем приложений, и запустите формирование этой выборки событий.

   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
- Kaspersky Security для виртуальных сред Легкий агент
- Справка Kaspersky Embedded Systems Security для Windows
- Справка Kaspersky Embedded Systems Security для Linux

Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows

После создания категорий для Контроля приложений, вы можете использовать их для настройки Контроля приложений в политиках Kaspersky Endpoint Security для Windows.

Чтобы настроить компонент Контроль приложений в политике Kaspersky Endpoint Security для Windows:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.

   Отобразится страница со списком политик.

2. Нажмите на политику **Kaspersky Endpoint Security для Windows**.

   Откроется окно свойств политики.

3. Перейдите в раздел **Параметры приложения** → **Контроль безопасности** → **Контроль приложений**.

   Отобразится окно **Контроль приложений** с параметрами компонента Контроль приложений.

4. Параметр **Контроль приложений** включен по умолчанию. Убедитесь, что переключатель **Контроль приложений Выключен** переведен в неактивное положение.

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 **OK**, чтобы сохранить параметры и закрыть окно **Списки запрещенных и разрешенных**.

17. Нажмите на кнопку **OK**, чтобы сохранить параметры и закрыть окно **Контроль приложений**.

18. Закройте окно с параметрами политики Kaspersky Endpoint Security для Windows.

    Компонент Контроль приложений настроен. После распространения политики на клиентские устройства запуск исполняемых файлов контролируется.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux
- Kaspersky Security для виртуальных сред Легкий агент
- Справка Kaspersky Embedded Systems Security для Windows
- Справка Kaspersky Embedded Systems Security для Linux

Получение и просмотр списка приложений, установленных на клиентских устройствах

Kaspersky Security Center выполняет инвентаризацию программного обеспечения, которое установлено на управляемых клиентских устройствах, работающих под управлением операционной системы Linux и Windows.

Агент администрирования составляет список приложений, установленных на устройстве, и передает список Серверу администрирования. Агенту администрирования требуется около 10–15 минут для обновления списка приложений.

Для клиентских устройств с операционной системой Windows Агент администрирования получает большую часть информации об установленных приложениях из реестра Windows. Для клиентских устройств с операционной системой Linux информацию об установленных приложениях Агент администрирования получает от диспетчеров пакетов.

Если на устройстве с операционной системной Linux обнаружено приложение из раздела **Реестр приложений**, в свойствах приложения отсутствует информация о связанных с ней исполняемых файлах.

Чтобы просмотреть список приложений, установленных на управляемых устройствах,

1. В главном окне приложения перейдите в раздел **Операции → Приложения сторонних производителей → Реестр приложений**.

   На странице отображается таблица с приложениями, установленными на управляемых устройствах. Выберите приложение, чтобы просмотреть свойства этого приложения, например: имя производителя, номер версии, список исполняемых файлов, список устройств, на которых установлено приложение, 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 столбцов** выберите столбцы, которые будут отображаться в таблице. Чтобы просмотреть тип операционной системы клиентских устройств, на которых установлено приложение, выберите столбец **Тип операционной системы**.

   - Нажмите на значок фильтрации ( ) в правом верхнем углу таблицы, укажите и примените критерий фильтрации в открывшемся меню.

     Отобразится отфильтрованная таблица установленных приложений.

Чтобы просмотреть список приложений, установленных на выбранном управляемом устройстве,

В главном окне приложения перейдите в раздел **Устройства** → **Управляемые устройства** → **<имя устройства>** → **Дополнительно** → **Реестр приложений**. В этом меню можно экспортировать список приложений в файлы форматов CSV или TXT.

Подробную информацию о Контроле приложений см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux
- Kaspersky Security для виртуальных сред Легкий агент
- Справка Kaspersky Embedded Systems Security для Windows
- Справка Kaspersky Embedded Systems 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". База данных создается автоматически при первом запуске задачи *Загрузка обновлений в хранилище Сервера администрирования*.

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 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** → **Приложения сторонних производителей** → **Теги приложений**.
2. Нажмите на кнопку **Добавить**.

   Отобразится окно создания тега.
3. Укажите тег.
4. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Новый созданный тег появляется в списке тегов приложения.

Изменение тегов приложений

Чтобы изменить тег приложения:

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Теги приложений**.
2. Установите флажок рядом с тегом, который вы хотите переименовать, и нажмите на кнопку **Изменить**.

   Откроется окно свойств тега.
3. Измените тег.
4. Нажмите на кнопку **OK**, 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** → **Приложения сторонних производителей** → **Реестр приложений**.
2. Выберите приложение, для которого требуется назначить теги.
3. Выберите вкладку **Теги**.

   На вкладке появятся все теги приложений, существующие на Сервере администрирования. Теги, назначенные выбранному приложению, отмечены флажками в 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** → **Приложения сторонних производителей** → **Реестр приложений**.

2. Выберите приложение, с которого требуется снять теги.

3. Выберите вкладку **Теги**.

   На вкладке появятся все теги приложений, существующие на Сервере администрирования. Теги, назначенные выбранному приложению, отмечены флажками в 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** → **Приложения сторонних производителей** → **Теги приложений**.

2. В списке выберите теги приложения, которые вы хотите удалить.

3. Нажмите на кнопку **Удалить**.

4. В появившемся окне нажмите на кнопку **ОК**.

Выбранный тег приложения удален. Удаленный тег автоматически снимается со всех приложений, которым он был назначен.

Мониторинг и отчеты

В этом разделе описаны функции мониторинга и работа с отчетами в Kaspersky Security Center. Эти функции позволяют получать сведения об инфраструктуре вашей сети, статусе защиты, а также статистику.

В процессе развертывания или во время работы Kaspersky Security Center можно настраивать функции мониторинга и параметры отчетов.

Сценарий: мониторинг и отчеты

В этом разделе представлен сценарий настройки мониторинга и отчетов в Kaspersky Security Center.

Предварительные требования

После развертывания Kaspersky Security Center в сети организации вы можете приступить к мониторингу состояния безопасности сети с помощью Kaspersky Security Center и к формированию отчетов.

Мониторинг и работа с отчетами в сети организации состоят из следующих этапов:

1. **Настройка переключения статусов устройств**

   Ознакомьтесь с параметрами статусов устройства в зависимости от конкретных условий. Изменяя эти параметры, вы можете изменить количество событий с уровнями важности *Критический* или *Предупреждение*. При настройке переключения состояний устройства убедитесь, что:

   - новые параметры не противоречат политикам информационной безопасности вашей организации;
   - вы можете своевременно реагировать на важные события безопасности в сети вашей организации.

2. **Настройка параметров уведомлений о событиях на клиентских устройствах**

   Инструкции:

   Настройка уведомлений (по электронной почте, по SMS или с помощью запуска исполняемого файла) о событиях на клиентских устройствах.

3. **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. **Выполнение рекомендуемых действий для критических и предупреждающих уведомлений**

   Инструкции:

   Выполните рекомендуемые действия для сети вашей организации.

5. **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.

6. **Нахождение незащищенных клиентских устройств**

   Инструкции:

   - Просмотр виджета Новые устройства.
   - Генерация и просмотр отчета Отчет о развертывании защиты.

7. **Проверка защиты клиентских устройств**

   Инструкции:

   - Генерация и просмотр отчета из категорий Состояние защиты и Статистика угроз.
   - Запуск и просмотр выборки событий Критическое.

8. **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:

   - Расчет места в базе данных.
   - Ограничение максимального количества событий.

9. **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 Web Console предоставляет следующие виды мониторинга и отчетов в сети вашей организации:

- Панель мониторинга
- Отчеты
- Выборки событий
- Уведомления

Панель мониторинга

Панель мониторинга позволяет контролировать состояние безопасности в сети вашей организации с помощью графического представления информации.

Отчеты

Отчеты позволяют вам получить подробную числовую информацию о безопасности сети вашей организации для сохранения этой информации в файл, отправки ее по электронной почте и печати.

Выборки событий

Выборки событий предназначены для просмотра на экране именованных наборов событий, которые выбраны из базы данных Сервера администрирования. Эти типы событий сгруппированы по следующим категориям:

- Уровень важности: **Критические события**, **Отказы функционирования**, **Предупреждения** и **Информационные события**.
- Время: **Последние события**.
- Тип: **Запросы пользователей** и **События аудита**.

Вы можете создавать и просматривать определенные пользователем выборки событий на основе параметров, доступных для настройки в интерфейсе Kaspersky Security Center Web Console.

Уведомления

Уведомления предназначены для оповещения о событиях и для того, чтобы помочь вам увеличить скорость ваших ответов на эти события, выполнив рекомендуемые действия, которые вы считаете подходящими.

Панель мониторинга и виджеты

В этом разделе содержится информация о панели мониторинга и виджетах, представленных в панели мониторинга. Раздел содержит инструкции по управлению виджетами и настройке виджетов.

Использование панели мониторинга

Панель мониторинга позволяет контролировать состояние безопасности в сети вашей организации с помощью графического представления информации.

Панель мониторинга доступна в Kaspersky Security Center Web Console в разделе **Мониторинг и отчеты** → **Панель мониторинга**.

В панели мониторинга представлены настраиваемые виджеты. Вы можете выбрать большое количество различных виджетов, представленных в виде круговых диаграмм, таблиц, графиков, гистограмм и списков. Информация, отображаемая в виджетах, обновляется автоматически, период обновления составляет от одной до двух минут. Интервал времени между обновлениями зависит от типа виджета. Вы можете обновить данные виджета вручную с помощью меню, в любое время.

По умолчанию виджеты включают информацию о событиях, хранящихся в базе данных Сервера администрирования.

Kaspersky Security Center Web Console имеет по умолчанию набор виджетов для следующих категорий:

- **Состояние защиты**
- **Развертывание**
- **Обновление**
- **Статистика угроз**
- **Другие**

Некоторые виджеты имеют текст со ссылками. Чтобы просмотреть подробную информацию, перейдите по ссылке.

При настройке панели мониторинга можно добавлять необходимые виджеты, скрывать виджеты, а также менять внешний вид или размер виджетов, перемещать виджеты и изменять параметры виджетов.

Добавление виджета на информационную панель

Чтобы добавить виджет на информационную панель:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
2. Нажмите на кнопку **Добавить или восстановить веб-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 и отчеты** → **Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с виджетом, который требуется удалить.
3. Выберите **Скрыть веб-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 и отчеты** → **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 и отчеты** → **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 и отчеты** → **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 веб-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 и отчеты** → **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 (например, это может быть топ-менеджер). Когда у пользователя включен этот режим, у пользователя отображается только панель мониторинга с предопределенным набором виджетов. Таким образом, пользователь может просматривать указанную в виджетах статистику, например, состояние защиты всех управляемых устройств, количество недавно обнаруженных угроз или список наиболее частых угроз в сети.

При работе пользователя в режиме Просмотра только панели мониторинга применяются следующие ограничения:

- Главное меню не отображается, поэтому пользователь не может изменить параметры защиты сети.
- Пользователь не может выполнять действия с виджетами, например, добавлять или скрывать их. Поэтому нужно разместить в панели мониторинга все необходимые пользователю виджеты и настроить их, например, задать правило подсчета объектов или указать период.

Вы не можете назначить режим Просмотра только панели мониторинга себе. Если вы хотите работать в этом режиме, обратитесь к системному администратору, поставщику услуг (MSP) или пользователю с правами **Изменение списков управления доступом объектов** в функциональной области **Общие функции: Права пользователя**.

Настройка режима Просмотра только панели мониторинга

Перед началом настройки режима Просмотра только панели мониторинга убедитесь, что выполнены следующие предварительные требования:

- У вас есть право **Изменение списков управления доступом объектов** в функциональной области **Общие функции: Права пользователя**. Если у вас нет этого права, вкладка для настройки режима будет отсутствовать.
- Пользователь с правом **Чтение** в области **Общие функции: Базовая функциональность**.

Если в вашей сети выстроена иерархия Серверов администрирования, для настройки режима Просмотра только панели мониторинга перейдите на тот Сервер, на котором учетная запись пользователя доступна на вкладке **Пользователи** в разделе **Пользователи и роли → Пользователи и группы**. Это может быть главный Сервер или физический подчиненный Сервер. На виртуальном Сервере администрирования настроить режим Просмотра только панели мониторинга невозможно.

Чтобы настроить режим Просмотра только панели мониторинга:

1. В главном окне приложения перейдите в раздел **Пользователи и роли → Пользователи и группы** и выберите вкладку **Пользователи**.
2. Нажмите на имя учетной записи пользователя, для которой вы хотите настроить панель инструментов с виджетами.
3. В открывшемся окне свойств учетной записи выберите вкладку **Панель мониторинга**.

   На открывшейся вкладке отображается та же панель мониторинга, что и для пользователя.
4. Если параметр **Отображать режим Просмотра только панели мониторинга** включен, выключите его переключателем.

   Когда этот параметр включен, также невозможно изменить панель мониторинга. После выключения параметра можно управлять виджетами.
5. Настройте внешний вид панели мониторинга. Набор виджетов, подготовленный на вкладке **Панель мониторинга**, доступен пользователю с настраиваемой учетной записью. Пользователь с такой учетной записью не может изменять какие-либо параметры или размер виджетов, добавлять или удалять виджеты с панели мониторинга. Поэтому настройте их под пользователя, чтобы он мог просматривать статистику защиты сети. Для этого на вкладке **Панель мониторинга** можно выполнять те же действия с виджетами, что и в разделе **Мониторинг и отчеты → Панель мониторинга**:
   - Добавлять виджеты в панель мониторинга.
   - Скрывать виджеты, которые не нужны пользователю.
   - Перемещать виджеты в определенном порядке.
   - Изменять размер или внешний вид виджетов.
   - Изменять параметры виджетов.

6. Переключите переключатель, чтобы включить параметр **Отображать режим Просмотра только панели мониторинга**.

   После этого пользователю доступна только панель мониторинга. Пользователь может просматривать статистику, но не может изменять параметры защиты сети и внешний вид панели мониторинга. Так как вам отображается та же панель мониторинга, что и для пользователя, вы также не можете изменить панель мониторинга.

   Если оставить этот параметр выключенным, у пользователя отображается главное меню, поэтому он может выполнять различные действия в Kaspersky Security Center, 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 под настраиваемой учетной записью и просматривать статистику защиты сети в режиме Просмотра только панели мониторинга.

Отчеты администрирования и защиты

В этом разделе описывается, как использовать отчеты, управлять шаблонами пользовательских отчетов, использовать шаблоны для создания отчетов и создавать задачи рассылки отчетов.

Использование отчетов

Отчеты позволяют вам получить подробную числовую информацию о безопасности сети вашей организации для сохранения этой информации в файл, отправки ее по электронной почте и печати.

Отчеты доступны в Kaspersky Security Center Web Console в разделе **Мониторинг и отчеты** → **Отчеты**.

По умолчанию отчеты включают информацию за последние 30 дней.

Kaspersky Security Center имеет по умолчанию набор отчетов для следующих категорий:

- **Состояние защиты**
- **Развертывание**
- **Обновление**
- **Статистика угроз**
- **Другие**

Вы можете создавать пользовательские шаблоны отчетов, 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 и отчеты** → **Отчеты**.
2. Нажмите на кнопку **Добавить**.

   В результате запустится мастер создания шаблона отчета. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Введите название отчета и выберите тип отчета.
4. На шаге мастера **Область действия** выберите набор клиентских устройств (групп администрирования, выборок устройств или всех сетевых устройств), данные о которых будут отображаться в отчетах, сформированных на основе этого шаблона.
5. На шаге мастера **Период отчета** укажите период, за который будет формироваться отчет. Доступные значения:

   - между двумя указанными датами;
   - от указанной даты до даты создания отчета;
   - от даты создания отчета минус указанное количество дней до даты создания отчета.

   В некоторых отчетах эта страница может не отображаться.
6. Нажмите на кнопку **ОК**, чтобы завершить работу мастера.
7. Выполните одно из следующих действий:

   - Нажмите на кнопку **Сохранить и запустить**, чтобы сохранить новый шаблон отчета и запустить формирование отчета на его основе.

     Шаблон отчета будет сохранен. Отчет будет сформирован.
   - Нажмите на кнопку **Сохранить**, чтобы сохранить новый шаблон отчета.

     Шаблон отчета будет сохранен.

Созданный шаблон можно использовать для формирования и просмотра отчетов.

Просмотр и изменение свойств шаблона отчета

Вы можете просматривать и изменять основные свойства шаблона отчета, например, имя шаблона отчета или поля, отображаемые в отчете.

Чтобы просмотреть и изменить свойства шаблона отчета:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Отчеты**.
2. Установите флажок напротив шаблона отчета, свойства которого вы хотите просмотреть и изменить.

   В качестве альтернативы можно сначала сформировать отчет, 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.

       Записи отчета сначала сортируются в соответствии с правилами, указанными в разделе **Столбцы → Детальные данные** свойств шаблона отчета, а затем сохраняется только первая часть результирующих записей. В заголовке таблицы с подробными данными отчета показано отображаемое количество записей и общее количество записей, соответствующее другим параметрам шаблона отчета.

       Если этот параметр выключен, в таблице с подробными данными отчета отображаются все записи. Не рекомендуется выключать этот параметр. Ограничение количества отображаемых записей отчета снижает нагрузку на систему управления базами данных и время, требуемое для формирования и экспорта отчета. В некоторых отчетах содержится слишком большое количество записей. В таких случаях просмотр и анализ всех записей может оказаться слишком трудоемким. Также на устройстве при формировании такого отчета может закончиться память. Это может привести к тому, что вам не удастся просмотреть отчет.

       По умолчанию параметр включен. По умолчанию указано значение 1000.

     - **Группа**

       Нажмите на кнопку **Параметры**, чтобы изменить набор клиентских устройств, для которых создается отчет. Для некоторых типов отчетов кнопка может быть недоступна. Реальные данные зависят от значений параметров, указанных при создании шаблона отчета.

     - **Период**

       Нажмите на кнопку **Параметры**, чтобы изменить период, за который будет сформирован отчет. Для некоторых типов отчетов кнопка может быть недоступна. Доступные значения:

       - между двумя указанными датами;
       - от указанной даты до даты создания отчета;
       - от даты создания отчета минус указанное количество дней до даты создания отчета.

     - **Включать данные подчиненных и виртуальных Серверов администрирования**

       Если этот параметр включен, отчет содержит информацию с подчиненных и виртуальных Серверов администрирования, которые подчинены Серверу администрирования, для которого создан шаблон отчета.

Выключите этот параметр, если вы хотите просматривать данные только текущего Сервера администрирования.

По умолчанию параметр включен.

- **До уровня вложенности**

  Отчет содержит данные подчиненных и виртуальных Серверов администрирования, которые находятся под текущим Сервером администрирования на уровне вложенности ниже или равном указанному значению.

  По умолчанию указано значение 1. Вы можете изменить это значение, если вы хотите видеть в отчете информацию Серверов администрирования, расположенных на более низких уровнях вложенности дерева.

- **Интервал ожидания данных (мин)**

  Сервер администрирования, для которого создан шаблон отчета, ожидает данные от подчиненных Серверов администрирования в течение указанного времени для создания отчета. Если данные не получены от подчиненного Сервера администрирования в течение указанного интервала времени, отчет запускается в любом случае. Вместо фактических данных в отчете отображаются данные, полученные из кеша (если включен параметр **Кешировать данные с подчиненных Серверов администрирования**), или в противном случае **N/A** (Недоступно).

  По умолчанию время ожидания составляет 5 минут.

- **Кешировать данные с подчиненных Серверов администрирования**

  Подчиненные Серверы администрирования регулярно передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Переданные данные хранятся в кеше.

  Если Сервер администрирования не может получить данные подчиненного Сервера администрирования во время генерации отчета, в отчете отобразятся данные из кеша. В этом случае отображается дата, когда данные были переданы в кеш.

  Включение этого параметра позволяет просматривать информацию, полученную от подчиненных Серверов администрирования, даже если невозможно получить актуальные данные. Однако отображаемые данные могут быть устаревшими.

  По умолчанию параметр выключен.

- **Период обновления данных в кеше (ч)**

  Подчиненные Серверы администрирования регулярно передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Вы можете указать этот период в часах. Если установлено значение 0, данные передаются только во время генерации отчета.

  По умолчанию указано значение 0.

- **Передавать подробную информацию с подчиненных Серверов администрирования**

  В созданном отчете таблица с подробными данными включает информацию с подчиненных Серверов администрирования главного Сервера администрирования, для которого создан шаблон отчета.

  Если этот параметр включен, то замедляется создание отчета и увеличивается трафик между Серверами администрирования. Однако вы можете просмотреть все данные в одном отчете.

  Чтобы не включать этот параметр, вы можете проанализировать данные отчета для нахождения неисправного подчиненного Сервера администрирования, а затем сформировать этот же отчет только для него.

  По умолчанию параметр выключен.

- Вкладка **Столбцы**

Выберите поля, которые будут отображаться в отчете. С помощью кнопок **Вверх** и **Вниз** измените порядок отображения полей. С помощью кнопок **Добавить** и **Изменить** укажите, будет ли информация в отчете фильтроваться или сортироваться по выбранным полям.

В разделе **Фильтры детальных полей** вы также можете нажать на кнопку **Преобразовать фильтры**, чтобы начать использовать расширенный формат фильтрации. Этот формат позволяет комбинировать условия фильтрации, указанные в различных полях, с помощью логического ИЛИ. После нажатия на кнопку **Преобразовать фильтры**, справа открывается панель. Нажмите на кнопку **Преобразовать фильтры**, подтверждающую отзыв лицензии. Теперь вы можете определить преобразованный фильтр с условиями из раздела **Детальные данные**, которые применяются с помощью логического ИЛИ.

Преобразование отчета в формат, поддерживающий сложные условия фильтрации, сделает его несовместимым с предыдущими версиями Kaspersky Security Center (11 и ниже). Также в преобразованном отчете не будет данных с подчиненных Серверов администрирования с несовместимыми версиями.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.
6. Закройте окно **Редактирование отчета <Название отчета>**.

Измененный шаблон отчета появится в списке шаблонов отчетов.

Экспорт отчета в файл

Вы можете экспортировать отчет в файл формата XML, HTML или PDF.

Чтобы экспортировать отчет в файл:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Отчеты**.
2. Установите флажок рядом с названием отчета, который требуется экспортировать в файл.
3. Нажмите на кнопку **Экспортировать отчет**.
4. В открывшемся окне измените имя файла отчета в поле **Имя**. По умолчанию имя файла совпадает с именем выбранного шаблона отчета.
5. Выберите тип файла отчета: XML, HTML или PDF.
6. Нажмите на кнопку **Экспортировать отчет**.

   Отчет будет загружен, в выбранном формате, в папку по умолчанию, на ваше устройство, или откроется стандартное окно **Сохранить как** в вашем браузере, чтобы вы могли сохранить файл в нужном вам месте.

Отчет будет сохранен в файл.

Генерация и просмотр отчета

Чтобы сформировать и просмотреть отчет:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. Нажмите на имя шаблона отчета, который вы хотите использовать для создания отчета.

   Отображается сгенерированный отчет с использованием выбранного шаблона.

Данные отчета отображаются в соответствии с языком локализации Сервера администрирования.

В 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 и отчеты** → **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**.

   d. Будут ли отчеты сохраняться в папку, будут ли перезаписываться сохраненные ранее отчеты в этой папке и будет ли использоваться отдельная учетная запись для доступа к папке (для папки общего доступа).

6. На шаге мастера **Настройка расписания 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 и отчеты** → **Отчеты**.

2. Установите флажки напротив шаблонов отчетов, которые требуется удалить.

3. Нажмите на кнопку **Удалить**.

4. В появившемся окне нажмите на кнопку **ОК**, чтобы подтвердить свой выбор.

Выбранные шаблоны отчетов будут удалены. Если эти шаблоны отчетов были включены в задачи рассылки отчетов, они также будут удалены из этих задач.

События и выборки событий

В этом разделе содержится информация о событиях и выборках событий, о типах событий, возникших в компонентах Kaspersky Security Center, и об управлении блокировкой частых событий.

О событиях Kaspersky Security Center

Kaspersky Security Center позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования.

Типы событий

В Kaspersky Security Center существуют следующие типы уведомлений:

- Общие события. Эти события возникают во всех управляемых приложениях "Лаборатории Касперского". Например, общее событие Вирусная атака. Общие события имеют строго определенные синтаксис и семантику. Общие события используются, например, в отчетах и панели мониторинга.
- Специфические события управляемых приложений "Лаборатории Касперского". Каждое управляемое приложение "Лаборатории Касперского" имеет собственный набор событий.

Источники событий

События могут генерироваться следующими приложениями:

- Компоненты приложения Kaspersky Security Center:
  - Сервер администрирования
  - Агент администрирования
  - Сервер iOS MDM
  - Сервер мобильных устройств Exchange ActiveSync
- Управляемые приложения "Лаборатории Касперского"

  Подробнее о событиях, генерируемых управляемыми приложениями "Лаборатории Касперского", см. в документации соответствующего приложения.

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.

Уровень важности события

Каждое событие имеет собственный уровень важности. В зависимости от условий возникновения, событию могут быть присвоены различные уровни важности. Существует четыре уровня важности событий:

- *Критическое событие* – событие, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.
- *Отказ функционирования* – событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы приложения или выполнения процедуры.

- *Предупреждение* – событие, не обязательно являющееся серьезным, однако указывающее на возможное возникновение проблемы в будущем. Чаще всего события относятся к Предупреждениям, если после их возникновения работа приложения может быть восстановлена без потери данных или функциональных возможностей.

- *Информационное сообщение* – событие, возникающее с целью информирования об успешном выполнении операции, корректной работе приложения или завершении процедуры.

Для каждого события задано время хранения, которое можно посмотреть или изменить в Kaspersky Security Center. Некоторые события не сохраняются в базе данных Сервера администрирования по умолчанию, поскольку для них установленное время хранения равно нулю. Во внешние системы можно экспортировать только те события, которые хранятся в базе данных Сервера администрирования не менее одного дня.

Использование выборок событий

Выборки событий предназначены для просмотра на экране именованных наборов событий, которые выбраны из базы данных Сервера администрирования. Эти типы событий сгруппированы по следующим категориям:

- Уровень важности: **Критические события**, **Отказы функционирования**, **Предупреждения** и **Информационные события**.

- Время: **Последние события**.

- Тип: **Запросы пользователей** и **События аудита**.

Вы можете создавать и просматривать определенные пользователем выборки событий на основе параметров, доступных для настройки в интерфейсе Kaspersky Security Center Web Console.

Выборки событий доступны в Kaspersky Security Center Web Console в разделе **Мониторинг и отчеты** → **Выборки событий**.

По умолчанию выборки событий включают информацию за последние семь дней.

Kaspersky Security Center имеет набор выборок (предопределенных) по умолчанию:

- События с разным уровнем важности:
  - **Критические события.**
  - **Отказ функционирования.**
  - **Предупреждения.**
  - **Информационные события.**
- **Запросы пользователей** (события управляемых приложений).
- **Последние события** (за последнюю неделю).
- **События аудита**.

Вы можете также создавать и настраивать дополнительные пользовательские выборки событий. В пользовательских выборках вы можете фильтровать события по свойствам устройств, в которых они возникли (по именам устройств, IP-диапазонам и группам администрирования), по типам событий и уровням важности, по названию приложения и компонента, а также по временному интервалу. Также можно включить результаты задачи в область поиска. Вы также можете использовать поле поиска, в котором можно ввести слово или несколько слов. Отображаются все события, содержащие любые введенные слова в любом месте их свойств (таких как имя события, описание, имя компонента).

Как для предопределенных выборок, так и для пользовательских выборок вы можете ограничить количество отображаемых событий или количество записей для поиска. Оба варианта влияют на время, за которое Kaspersky Security Center 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 и отчеты → Выборки событий**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Новая выборка событий** укажите параметры новой выборки событий. Параметры можно указать в нескольких разделах этого окна.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

   Откроется окно подтверждения.
5. Чтобы просмотреть результат выборки событий, установите флажок **Перейти к 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 и отчеты** → **Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется изменить.
3. Нажмите на кнопку **Свойства**.

   Откроется окно свойств выборки событий.
4. Отредактируйте свойства выборки событий.

   > Для стандартной выборки событий можно редактировать свойства только на следующих вкладках: **Общие** (за исключением имени выборки), **Время** и **Права доступа**.

   Для пользовательских выборок можно 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 и отчеты** → **Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется запустить.
3. Выполните одно из следующих действий:

   - Чтобы настроить сортировку для результатов выборки событий:

     a. Нажмите на кнопку **Изменить сортировку и запустить**.

     b. В отобразившемся окне **Изменить сортировку для выборки событий** укажите параметры сортировки.

     c. Нажмите на имя выборки.

   - В противном случае, если вы хотите просмотреть список событий так, как они хранятся на Сервере администрирования, нажмите на название выборки.

Отобразится результат выборки событий.

Экспорт выборки событий

Kaspersky Security Center позволяет сохранить выборку событий и ее параметры в файл KLO. Вы можете использовать файл KLO для импорта сохраненной выборки событий как в Kaspersky Security Center Windows, так и в Kaspersky Security Center Linux.

Обратите внимание, что можно удалять только определенные пользователем выборки событий. Набор выборок событий, заданных по умолчанию в Kaspersky Security Center (предопределенные выборки), не может быть сохранен в файл.

Чтобы экспортировать выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется экспортировать.

   Невозможно экспортировать несколько выборок событий одновременно. Если вы выберете более одной выборки, кнопка **Экспортировать** будет неактивна.
3. Нажмите на кнопку **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 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 и отчеты → Выборки событий**.
2. Нажмите на кнопку **Импортировать**, чтобы выбрать файл выборки событий, который вы хотите импортировать.
3. В открывшемся окне укажите путь к файлу KLO и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл выборки событий.

   Начнется обработка выборки событий.

Появится уведомление с результатами импорта. Если выборка событий импортирована, вы можете перейти по ссылке **Просмотреть сведения об импорте**, чтобы просмотреть свойства выборки.

После успешного импорта выборка событий отображается в списке выборок. Также импортируются параметры выборки событий.

Если имя новой импортированной выборки событий идентично имени существующей выборки, имя импортированной выборки расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Просмотр информации о событии

Чтобы просмотреть детальную информацию о событии:

1. Запустите выборку событий.
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 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.

Удаление событий

Чтобы удалить одно или несколько событий:

1. Запустите выборку событий.
2. Установите флажки рядом с требуемыми событиями.
3. Нажмите на кнопку **Удалить**.

   Выбранные события удалены и не могут быть восстановлены.

Удаление выборок событий

Можно удалять только пользовательские выборки событий. Предопределенные выборки событий невозможно удалить.

Чтобы удалить выборки событий:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Выборки событий**.
2. Установите флажки напротив выборок событий, которые требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **ОК**.

   Выборка событий будет удалена.

Настройка срока хранения события

Kaspersky Security Center позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования. Возможно, вам нужно хранить некоторые события в течение более длительного или более короткого периода, чем указано по умолчанию. Вы можете изменить срок хранения события по умолчанию.

Если вас не интересует сохранение каких-либо событий в базе данных Сервера администрирования, вы можете выключить соответствующий параметр в политике Сервера администрирования, политике приложения "Лаборатории Касперского" или в свойствах Сервера администрирования (только для событий Сервера администрирования). Это уменьшит количество типов событий в базе данных.

Чем больше срок хранения события, тем быстрее база данных достигает максимального размера. Однако более длительный срок хранения события позволяет выполнять задачи мониторинга и просматривать отчеты в течение более длительного периода.

Чтобы задать срок хранения события в базе данных Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.

2. Нажмите на название требуемой политики.

   Вы можете выбрать политику управляемого приложения "Лаборатории Касперского", Агента администрирования или Сервера администрирования. Для Сервера администрирования вы также можете настроить время хранения событий, нажав на значок параметров () рядом с именем нужного Сервера администрирования.

3. Выберите вкладку **Настройка событий**.

   Отображается раздел **Критическое** со списком связанных событий. При необходимости вы можете перейти в раздел **Отказ функционирования**, **Предупреждение** или **Информационное сообщение**.

4. В списке типов событий в правой панели перейдите по ссылке с названием события, срок хранения которого вы хотите изменить.

   В открывшемся окне в разделе **Регистрация событий** включите переключатель **Хранить в базе данных Сервера администрирования в течение (сут)**.

5. В поле редактирования под переключателем укажите количество дней для сохранения события.

6. Если вы не хотите сохранять событие в базе данных Сервера администрирования, выключите параметр **Хранить в базе данных Сервера администрирования в течение (сут)**.

> Если вы настраиваете события Сервера администрирования в окне свойств Сервера администрирования и если параметры событий заблокированы в политике Сервера администрирования Kaspersky Security Center, вы не сможете изменить значение срока хранения события.

7. Нажмите на кнопку **OK**, а затем после того как правая панель закроется, нажмите на кнопку **Сохранить**.

   Окно свойств политики закроется.

Теперь, когда Сервер администрирования получает и сохраняет события выбранного типа, они будут иметь измененный срок хранения. Сервер администрирования не изменяет срок хранения ранее полученных событий.

События компонентов Kaspersky Security Center

Каждый компонент Kaspersky Security Center имеет собственный набор типов событий. В этом разделе перечислены типы событий, которые происходят на Сервере администрирования Kaspersky Security Center, Агенте администрирования и Сервере iOS MDM. 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, когда вы настраиваете события и при их возникновении.
- **Идентификатор типа события**. Этот цифровой код используется при обработке событий с использованием инструментов анализа событий сторонних производителей.
- **Тип события** (буквенный код). Этот код используется при просмотре и обработке событий с использованием публичных представлений базы данных Kaspersky Security Center и при экспорте событий в SIEM-системы.
- **Описание**. Этот текст содержит описание ситуации при возникновении события и описание того, что вы можете сделать в этом случае.
- **Срок хранения по умолчанию**. Это количество дней, в течение которых событие хранится в базе данных Сервера администрирования и отображается в списке событий Сервера администрирования. После окончания этого периода событие удаляется. Если значение времени хранения события указано 0, такие события регистрируются, но не отображаются в списке событий Сервера администрирования. Если вы настроили хранение таких событий в журнале событий операционной системы, вы можете найти их там.

  Можно изменить время хранения событий:

  - Консоль администрирования: Настройка срока хранения события.
  - Kaspersky Security Center Web Console: Настройка срока хранения события.

Другие данные могут включать следующие поля:

- **event_id**: уникальный номер события в базе данных, генерируемый и присваиваемый автоматически. Его не нужно путать с **Идентификатором типа события**.
- **task_id**: идентификатор задачи, в результате выполнения которой возникло событие (если такая есть).
- **severity**: один из следующих уровней важности (в порядке возрастания важности):

  0) Недопустимый уровень важности.

  1) Информационное.

  2) Предупреждение.

  3) Ошибка.

  4) Критическое.

События Сервера администрирования

В этом разделе содержится информация о событиях Сервера администрирования.

Критические события Сервера администрирования

В таблице ниже приведены типы событий Сервера администрирования Kaspersky Security Center с уровнем важности **Критическое**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Если вы указали порт в окне свойств Сервера администрирования в Консоли администрирования, **Kaspersky Security Center публикует его метрики** и критические события, которые будет получать Prometheus (система мониторинга и оповещения). Prometheus получает метрики и критические события, а затем генерирует алерты для каждого события.

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

Критические события Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Лицензионное ограничение превышено	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Один раз в день Kaspersky Security Center проверяет, не 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 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
Файл ключа добавлен в список запрещенных	4124	KLSRV_LICENSE_BLACKLISTED	События этого типа возникают, если "Лаборатория Касперского" добавила код активации или файл ключа, который вы используете, в список запрещенных. Обратитесь в Службу технической поддержки для получения подробной информации.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Режим ограниченной функциональности	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	События этого типа возникают, если Kaspersky Security Center 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 (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. Вы не можете изменить количество дней. Если Сервер администрирования выключен, в указанный день окончания срока действия лицензии, событие не будет опубликовано до следующего дня. После окончания срока действия коммерческой лицензии, Kaspersky Security Center работает в режиме Базовой функциональности. Вы можете ответить на событие следующими способами: • Убедитесь, что резервный лицензионный ключ добавлен на Сервер администрирования. • Если вы используете подписку, продлите ее. Неограниченная подписка продлевается автоматически, если предоплата поставщику услуг была своевременно внесена.	180 дней
Срок действия сертификата истек	4132	KLSRV_CERTIFICATE_EXPIRED	События этого типа возникают, если истек срок действия клиентского сертификата на мобильных устройствах.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Срок действия сертификата Сервера администрирования истек.	6129	ServerCertificateExpired	События этого типа возникают, если истек срок действия сертификатов Сервера администрирования для мобильных устройств и для устройств с защитой на уровне UEFI в сети. Вам необходимо обновить сертификат, срок действия которого истек.	180 дней
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 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 типы событий Сервера администрирования Kaspersky Security Center с уровнем важности **Отказ функционирования**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

События отказа функционирования Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Ошибка времени выполнения	4125	KLSRV_RUNTIME_ERROR	События этого типа возникают из-за неизвестных проблем. Чаще всего это проблемы СУБД, проблемы с сетью и другие проблемы с программным и аппаратным обеспечением. Подробную информацию о событии можно найти в его описании.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Для одной из групп лицензионных приложений превышено ограничение числа установок	4126	KLSRV_INVLICPROD_EXCEDED	Сервер администрирования генерирует события такого типа периодически (каждый час). События этого типа возникают, если в Kaspersky Security Center вы управляете лицензионными ключами приложений сторонних производителей и если количество установок превысило заданное в лицензионном ключе приложения стороннего производителя ограничение. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите приложение стороннего производителя с устройств, на которых оно не используется. • Используйте лицензию стороннего производителя на большее количество устройств. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений. В группу лицензионных приложений входят приложения сторонних производителей, отвечающие заданным вами критериям.	180 дней
Не удалось выполнить 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
Не удалось выполнить копирование обновлений в заданную папку	4123	KLSRV_UPD_REPL_FAIL	События этого типа возникают, если обновления программного обеспечения копируются в общую папку (или папки). Вы можете ответить на событие следующими способами: • Проверить, имеет ли учетная запись пользователя, которая используется для получения доступа к папке (или папкам), права на запись. • Проверить, были ли изменены имя пользователя и/или пароль к папкам. • Проверить подключение к интернету, так как это может быть причиной события. Следуйте инструкциям по обновлению баз и модулей приложений.	180 дней
Нет свободного места на диске	4107	KLSRV_DISK_FULL	События этого типа возникают, если на жестком диске устройства, на котором установлен Сервер администрирования, заканчивается дисковое пространство. Освободите дисковое пространство на устройстве.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Общая папка недоступна	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	События этого типа возникают, если общая папка Сервера администрирования недоступна. Вы можете ответить на событие следующими способами: • Убедитесь, что Сервер администрирования (на котором находится общая папка) включен и доступен. • Проверьте, были ли изменены имя пользователя и/или пароль к папке. • Проверьте подключение к сети.	180 дней
База данных Сервера администрирования недоступна	4109	KLSRV_DATABASE_UNAVAILABLE	События этого типа возникают, если база Сервера администрирования становится недоступной. Вы можете ответить на событие следующими способами: • Проверьте, доступен ли удаленный сервер, на котором установлен SQL-сервер. • Просмотрите журналы событий СУБД и найдите причину недоступности базы Сервера администрирования. Например, из-за профилактических работ удаленный сервер с установленным SQL Server может быть недоступен.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Недостаточно места в базе данных Сервера администрирования	4110	KLSRV_DATABASE_FULL	События этого типа возникают, если нет свободного места в базе Сервера администрирования. Сервер администрирования не работает, если его база данных переполнена и дальнейшая запись в базу данных невозможна. Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие: • Вы используете SQL Server Express Edition: Проверьте в документации к SQL Server Express ограничение размера базы данных для используемой версии. Возможно, ваша база данных Сервера администрирования превысила ограничение размера базы данных. Ограничьте количество событий, хранящихся в базе данных Сервера администрирования. В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль приложений. Вы можете изменить параметры политики Kaspersky Endpoint Security для Windows, касающиеся хранения событий компонента Контроль приложений в базе данных Сервера администрирования. • Вы используете СУБД, отличную от SQL Server Express Edition: Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования. Сократите список событий для хранения в базе данных Сервера администрирования. Просмотрите информацию о выборе СУБД.	180 дней

События предупреждения Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Обнаружено получение частого события		KLSRV_EVENT_SPAM_EVENTS_DETECTED	События этого типа возникают, если Сервер администрирования регистрирует частые события на управляемом устройстве. Дополнительную информацию см. в следующих разделах: Блокировка частых событий.	90 дней
Лицензионное ограничение превышено	4098	KLSRV_EV_LICENSE_CHECK_100_110	Один раз в день Kaspersky Security Center 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 определяет правила генерации событий при превышении лицензионного ограничения.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Устройство долго не проявляет активности в сети	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	События этого типа возникают, если управляемое устройство неактивно в течение некоторого времени. Чаще всего это происходит, когда управляемое устройство выводится из эксплуатации. Вы можете ответить на событие следующими способами: • Удалите устройство из списка управляемых устройств вручную. • Укажите интервал, по истечении которого создается событие **Устройство долго не проявляет активности в сети** с помощью Консоли администрирования или с помощью Kaspersky Security Center Web Console. • Укажите интервал, по истечении которого устройство автоматически удаляется из группы с помощью Консоли администрирования или Kaspersky Security Center Web Console.	90 дней
Конфликт имен устройств	4102	KLSRV_EVENT_HOSTS_CONFLICT	События этого типа возникают, если Сервер администрирования рассматривает два или более управляемых устройства как одно устройство. Чаще всего это происходит, когда клонированный жесткий диск использовался для развертывания приложений на управляемых устройствах и без переключения Агента администрирования в режим клонирования выделенного диска на эталонном устройстве. Чтобы избежать этой проблемы, перед клонированием жесткого диска этого устройства переключите Агент администрирования в режим клонирования диска на эталонном устройстве.	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 превышено ограничение числа установок	4127	KLSRV_INVLICPROD_FILLED	События этого типа возникают, если количество установок приложений сторонних производителей, включенных в группу лицензионных приложений, достигает 90% от максимально допустимого значения, указанного в свойствах лицензионного ключа. Вы можете ответить на событие следующими способами: • Если приложение стороннего производителя не используется на каких-то управляемых устройствах, удалите приложение с этих устройств. • Если вы ожидаете, что количество установок для приложения стороннего производителя превысит разрешенное ограничение в ближайшем будущем, рассмотрите возможность получения лицензии приложения стороннего производителя на большее количество устройств заранее. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений.	90 дней
Сертификат запрошен	4133	KLSRV_CERTIFICATE_REQUESTED	События этого типа возникают, если не удается автоматически перевыпустить сертификат для Управления мобильными устройствами. Ниже приведены возможные причины событий и соответствующие действия по реагированию на событие: • Автоматический перевыпуск был инициирован для сертификата, для которого параметр **Автоматически перевыпускать сертификат, если это возможно**. 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 сертификата истекает.	6128	ServerCertificateExpiresSoon	События этого типа возникают, если истек срок действия сертификатов Сервера администрирования для мобильных устройств и для устройств с защитой на уровне UEFI в сети. Вам необходимо обновить сертификат, срок действия которого истек.	90 дней
Срок действия APNs-сертификата истек	4135	KLSRV_APN_CERTIFICATE_EXPIRED	События этого типа происходят, если истекает срок действия APNs-сертификата. Вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM.	Не хранится
Срок действия APNs-сертификата истекает	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	События этого типа возникают, если до истечения срока действия APNs-сертификата остается менее 14 дней. При истечении срока действия APNs-сертификата, вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM. Рекомендуется запланировать обновление APNs-сертификата до истечения срока его действия.	Не хранится

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось отправить FCM-сообщение на мобильное устройство	4138	KLSRV_GCM_DEVICE_ERROR	События этого типа возникают, если Управление мобильными устройствами настроено на использование 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 Firebase (см. главу "Downstream message error response codes").	90 дней
HTTP-ошибка при отправке FCM-сообщения на FCM-сервер	4139	KLSRV_GCM_HTTP_ERROR	События этого типа возникают, если Управление мобильными устройствами настроено на использование 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 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

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось отправить FCM-сообщение на FCM-сервер	4140	KLSRV_GCM_GENERAL_ERROR	События этого типа возникают из-за непредвиденных ошибок на стороне Сервера администрирования при работе с HTTP-протоколом Firebase Cloud Messaging. Прочтите информацию в описании события и отреагируйте соответствующим образом. Если вы не можете найти решение проблемы самостоятельно, рекомендуем вам обратиться в Службу технической поддержки "Лаборатории Касперского".	90 дней
Мало свободного места на жестком диске	4105	KLSRV_NO_SPACE_ON_VOLUMES	События этого типа возникают, если на устройстве, на котором установлен Сервер администрирования, почти закончилось дисковое пространство. Освободите дисковое пространство на устройстве.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Мало свободного места в базе Сервера администрирования	4106	KLSRV_NO_SPACE_IN_DATABASE	События этого типа возникают, если свободное место в базе Сервера администрирования ограничено. Если вы не устраните эту проблему, скоро база данных Сервера администрирования достигнет своей емкости и Сервер администрирования не будет работать. Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие. Вы используете SQL Server Express Edition: • Проверьте в документации к SQL Server Express ограничение размера базы данных для используемой версии. Возможно, ваша база данных Сервера администрирования достигла ограничения размера базы данных. • Ограничьте количество событий, хранящихся в базе данных Сервера администрирования. • В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль приложений. Вы можете изменить параметры политики Kaspersky Endpoint Security для Windows, касающиеся хранения событий компонента Контроль приложений в базе данных Сервера администрирования. Вы используете СУБД, отличную от SQL Server Express Edition: • Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования. • Сократите список событий для хранения в базе данных Сервера администрирования. Просмотрите информацию о выборе СУБД.	90 дней
Разорвано соединение с подчиненным Сервером администрирования	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	События этого типа возникают при разрыве соединения с подчиненным Сервером администрирования. Прочтите журнал событий Kaspersky Event Log на устройстве, на котором установлен подчиненный Сервер администрирования, и отреагируйте соответствующим образом.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Разорвано соединение с главным Сервером администрирования	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	События этого типа возникают при разрыве соединения с главным Сервером администрирования. Прочтите журнал событий Kaspersky Event Log на устройстве, на котором установлен главный Сервер администрирования, и отреагируйте соответствующим образом.	90 дней
Зарегистрированы новые обновления модулей 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 Консоли администрирования или 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

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Аудит (Не удалось выполнить тестовое подключение к SIEM-серверу)	5120	KLAUD_EV_SIEM_TEST_FAILED	События этого типа возникают, если не удалось подключится к SIEM-серверу.	30 дней
Не удалось выписать сертификат автоматически		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	Это событие возникает в случае ошибки создания клиентского сертификата для мобильного устройства (устройства, работающего по мобильному протоколу).	90 дней

Информационные события Сервера администрирования

В таблице ниже приведены события Сервера 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. 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	Срок хранения по умолчанию	Комментарий
Лицензионный ключ использован более чем на 90%	4097	KLSRV_EV_LICENSE_CHECK_90	30 дней	
Обнаружено новое устройство	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 дней	
Устройство автоматически добавлено в группу	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 дней	
Устройство было автоматически перемещено с помощью правила	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 дней	
Устройство удалено из группы: долгое отсутствие активности в сети	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 дней	
Для одной из групп лицензионных приложений число разрешенных установок исчерпано более чем на 95%	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 дней	
Появились файлы для отправки на анализ в "Лабораторию Касперского"	4131	KLSRV_APS_FILE_APPEARED	30 дней	
Идентификатор экземпляра FCM мобильного устройства изменен	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 дней	
Обновления успешно скопированы в заданную папку	4122	KLSRV_UPD_REPL_OK	30 дней	

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию	Комментарий
Установлено соединение с подчиненным Сервером администрирования	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 дней	
Установлено соединение с главным Сервером администрирования	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 дней	
Базы обновлены	4144	KLSRV_UPD_BASES_UPDATED	30 дней	
Аудит: Подключение к Серверу администрирования	4147	KLAUD_EV_SERVERCONNECT	30 дней	События этого типа возникают при подключении пользователя к Серверу администрирования с помощью Консоли администрирования или Kaspersky Security Center Web Console. Такие события включают информацию об IP-адресе устройства, на котором установлена Консоль администрирования на основе консоли Microsoft Management Console (MMC) или Сервер Kaspersky Security Center Web Console.
Аудит: Изменение объекта	4148	KLAUD_EV_OBJECTMODIFY	30 дней	Это событие отслеживает изменения в следующих объектах: • группах администрирования; • группах безопасности; • пользователях; • инсталляционных пакетах; • задачах; • политиках; • Серверах; • виртуальных Серверах.
Аудит: Изменение статуса объекта	4150	KLAUD_EV_TASK_STATE_CHANGED	30 дней	Например, это событие возникает, если задача завершилась ошибкой.
Аудит: Изменение параметров группы	4149	KLAUD_EV_ADMGROUP_CHANGED	30 дней	
Аудит: Подключение к Серверу администрирования было прервано	4151	KLAUD_EV_SERVERDISCONNECT	30 дней	
Аудит: Свойства объекта были изменены	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 дней	Это событие отслеживает изменения в следующих параметрах: • пользователь; • лицензия; • Сервер; • виртуальный Сервер.

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию	Комментарий
Аудит: Права пользователя были изменены	4153	KLAUD_EV_OBJECTACLMODIFIED	30 дней	
Аудит: Импорт или экспорт ключей шифрования с Сервера администрирования	5100	KLAUD_EV_DPEKEYSEXPORT	30 дней	
Аудит: Проверка подключения к SIEM-серверу выполнена успешно	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 дней	События этого типа возникают при успешном подключении к SIEM-серверу.
Резервный сертификат создан		ServerReserveCertificateCreated	30 дней	События этого типа возникают, если сертификат Сервера администрирования создан.
Сертификат обновлен		ServerCertificateRenewed	30 дней	События этого типа возникают, если сертификат Сервера администрирования был обновлен.

События **Резервный сертификат создан** и **Сертификат обновлен** автоматически публикуются Сервером администрирования и отображаются в Консоли администрирования только при выполнении соответствующих этим событиям операций для сертификатов Сервера администрирования для мобильных устройств и устройств с защитой на уровне UEFI.

События Агента администрирования

В этом разделе содержится информация о событиях Агента администрирования.

События отказа функционирования Агента администрирования

В таблице ниже приведены типы событий 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 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
Управление учетными записями: ошибки	7723	KLNAG_EV_USR_MNG_ERR	Общее событие предупреждения.	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
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

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
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
Обнаружен файл sudoers, который не соответствует референсному значению	7724	KLNAG_EV_SUDOER_DIFFERENT	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	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
Новое устройство добавлено	7708	KLNAG_EV_DEVICE_ARRIVAL	30 дней
Устройство удалено	7709	KLNAG_EV_DEVICE_REMOVE	30 дней
Обнаружено новое устройство	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 дней
Устройство авторизовано	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 дней
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

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
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

События Сервера iOS MDM

В этом разделе содержится информация о событиях Сервера iOS MDM.

События отказа функционирования Сервера iOS MDM

В таблице ниже приведены события Сервера iOS MDM 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.

События отказа функционирования Сервера iOS MDM

Отображаемое имя типа события	Тип события	Срок хранения по умолчанию
Не удалось запросить список профилей	PROFILELIST_COMMAND_FAILED	30 дней
Не удалось установить профиль	INSTALLPROFILE_COMMAND_FAILED	30 дней
Не удалось удалить профиль	REMOVEPROFILE_COMMAND_FAILED	30 дней
Не удалось запросить список provisioning-профилей	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 дней
Не удалось установить provisioning-профиль	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 дней
Не удалось удалить provisioning-профиль	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 дней
Не удалось запросить список цифровых сертификатов	CERTIFICATELIST_COMMAND_FAILED	30 дней
Не удалось запросить список установленных приложений	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 дней
Не удалось запросить общую информацию о мобильном устройстве	DEVICEINFORMATION_COMMAND_FAILED	30 дней
Не удалось запросить информацию о безопасности	SECURITYINFO_COMMAND_FAILED	30 дней
Не удалось заблокировать мобильное устройство	DEVICELOCK_COMMAND_FAILED	30 дней
Не удалось очистить пароль	CLEARPASSCODE_COMMAND_FAILED	30 дней
Не удалось удалить данные мобильного устройства	ERASEDEVICE_COMMAND_FAILED	30 дней
Не удалось установить приложение	INSTALLAPPLICATION_COMMAND_FAILED	30 дней

Отображаемое имя типа события	Тип события	Срок хранения по умолчанию
Не удалось установить код погашения для приложения	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 дней
Не удалось запросить список управляемых приложений	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 дней
Не удалось удалить управляемое приложение	REMOVEAPPLICATION_COMMAND_FAILED	30 дней
Параметры роуминга отклонены	SETROAMINGSETTINGS_COMMAND_FAILED	30 дней
Произошла ошибка в работе приложения	PRODUCT_FAILURE	30 дней
Результат выполнения команды содержит неверные данные	MALFORMED_COMMAND	30 дней
Не удалось отправить уведомление (Push Notification)	SEND_PUSH_NOTIFICATION_FAILED	30 дней
Не удалось отправить команду	SEND_COMMAND_FAILED	30 дней
Устройство не найдено	DEVICE_NOT_FOUND	30 дней

События предупреждения Сервера iOS MDM

В таблице ниже приведены события Сервера iOS MDM 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 Сервера iOS MDM

Отображаемое имя типа события	Тип события	Срок хранения по умолчанию
Попытка подключения заблокированного мобильного устройства	INACTICE_DEVICE_TRY_CONNECTED	30 дней
Профиль удален	MDM_PROFILE_WAS_REMOVED	30 дней
Попытка повторного использования клиентского сертификата	CLIENT_CERT_ALREADY_IN_USE	30 дней
Обнаружено неактивное устройство	FOUND_INACTIVE_DEVICE	30 дней
Требуется код погашения	NEED_REDEMPTION_CODE	30 дней
Профиль, входящий в состав политики, удален с устройства	UMDM_PROFILE_WAS_REMOVED	30 дней

Информационные события Сервера iOS MDM

В таблице ниже приведены события Сервера iOS MDM 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 Сервера iOS MDM

Отображаемое имя типа события	Тип события	Срок хранения по умолчанию
Подключено новое мобильное устройство	NEW_DEVICE_CONNECTED	30 дней
Запрос списка профилей выполнен успешно	PROFILELIST_COMMAND_SUCCESSFULL	30 дней
Установка профиля выполнена успешно	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 дней
Удаление профиля выполнено успешно	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 дней

Отображаемое имя типа события	Тип события	Срок хранения по умолчанию
Запрос списка provisioning-профилей выполнен успешно	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 дней
Установка provisioning-профиля выполнена успешно	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 дней
Удаление provisioning-профиля выполнено успешно	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 дней
Запрос списка цифровых сертификатов выполнен успешно	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 дней
Запрос списка установленных приложений выполнен успешно	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 дней
Запрос общей информации о мобильном устройстве выполнен успешно	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 дней
Запрос информации о безопасности выполнен успешно	SECURITYINFO_COMMAND_SUCCESSFULL	30 дней
Мобильное устройство успешно заблокировано	DEVICELOCK_COMMAND_SUCCESSFULL	30 дней
Очистка пароля выполнена успешно	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 дней
Данные удалены с мобильного устройства	ERASEDEVICE_COMMAND_SUCCESSFULL	30 дней
Установка приложения выполнена успешно	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 дней
Установка кода погашения для приложения прошла успешно	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 дней
Запрос списка управляемых приложений выполнен успешно	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 дней
Удаление управляемого приложения выполнено успешно	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 дней
Параметры роуминга применены успешно	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 дней

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.

Использование уведомлений

Уведомления предназначены для оповещения о событиях и для того, чтобы помочь вам увеличить скорость ваших ответов на эти события, выполнив рекомендуемые действия, которые вы считаете подходящими.

В зависимости от выбранного способа уведомления доступны следующие типы уведомлений:

- экранные уведомления;
- уведомление по SMS;
- уведомление по электронной почте;
- уведомление запуском исполняемого файла или скрипта.

Экранные уведомления

Экранные уведомления предупреждают вас о событиях, сгруппированных по уровням важности (*Критическое уведомление*, *Предупреждающие уведомление*, и *Информационное уведомление*).

Экранные уведомления могут иметь один из двух статусов:

- *Просмотрено*. Это означает, что вы выполнили рекомендованное действие для уведомления или вы назначили этот статус для уведомления вручную.
- *Не просмотрено*. Это означает, что вы не выполнили рекомендуемое действие для уведомления или не назначили этот статус для уведомления вручную.

По умолчанию в список уведомлений входят уведомления со статусом *Не просмотрено*.

Вы можете контролировать сеть вашей организации, просматривая уведомления на экране и отвечая на них в режиме реального времени.

Уведомления по электронной почте, SMS и запуском исполняемого файла или скрипта

Kaspersky Security Center позволяет вам контролировать сеть вашей организации, отправляя уведомления о событиях, которые вы считаете важными. Для любого события вы можете настроить уведомления по электронной почте, SMS или запустив исполняемый файл или скрипт.

Получив уведомление по SMS или по электронной почте, вы можете принять решение о своем ответе на событие. Этот ответ должен быть наиболее подходящим для сети вашей организации. Запустив исполняемый файл или скрипт, вы заранее определяете ответ на событие. Вы также можете рассмотреть запуск исполняемого файла или скрипта в качестве основного ответа на событие. После запуска исполняемого файла вы можете предпринять другие шаги для ответа на событие.

Просмотр экранных уведомлений

Вы можете просматривать экранные уведомления тремя способами:

- В разделе **Мониторинг и отчеты → Уведомления**. Здесь вы можете просмотреть уведомления, относящиеся к предопределенным категориям.
- В отдельном окне, которое можно открыть независимо от того, какой раздел вы используете в данный момент. В этом случае вы можете отметить уведомления как просмотренные.
- В виджете **Уведомления, выбранные по уровню важности** в разделе **Мониторинг и отчеты → Панель мониторинга**. В этом виджете вы можете просматривать только уведомления с уровнями важности *Критическое* и *Предупреждение*.

Вы можете выполнять действия, например, вы можете ответить на событие.

Чтобы просмотреть уведомления предопределенной категории:

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Уведомления**.

   На левой панели выбрана категория **Все уведомления**, а справа отображаются все уведомления.

2. На левой панели выберите одну из следующих категорий:

   - **Развертывание.**
   - **Устройства.**
   - **Защита.**
   - **Обновления** (сюда входят уведомления о доступных для загрузки приложениях "Лаборатории Касперского" и уведомления о загруженных обновлениях антивирусных баз).
   - **Защита от эксплойтов.**

- **Сервер администрирования** (это уведомление включает в себя события, относящиеся только к Серверу администрирования).

- **Полезные ссылки** (сюда входят ссылки на ресурсы "Лаборатории Касперского", например, ссылка на Службу технической поддержки "Лаборатории Касперского", на форум "Лаборатории Касперского", на страницу продления лицензии или на Вирусную энциклопедию).

В списке уведомлений отобразится выбранная категория. Список содержит следующее:

- Значок, относящийся к теме уведомления: развертывание (), защита (), обновления (), управление устройствами (), Защита от эксплойтов (), Сервер администрирования ().

- Уровень важности уведомления. Отображаются уведомления со следующими уровнями важности: **Критические уведомления** (), **Предупреждающие уведомления** (), **Информационные уведомления**. Уведомления в списке сгруппированы по уровню важности.

- **Уведомление**. Здесь содержится описание уведомления.

- **Действие**. Здесь содержится ссылка на быстрое действие, которое рекомендуется выполнить. Например, по этой ссылке вы можете перейти к хранилищу и установить приложение безопасности на устройства, просмотреть список устройств или список событий. После того как вы выполнили рекомендуемое действие для уведомления, этому уведомлению присваивается статус *Просмотрено*.

- **Зарегистрированный статус**. Здесь содержится количество дней или часов, прошедших с даты регистрации уведомления на Сервере администрирования.

Чтобы просмотреть экранные уведомления в отдельном окне по уровню важности:

1. Нажмите на значок флага () в правом верхнем углу Kaspersky Security Center Web Console.

   Если около значка флажка есть красная точка, значит, есть непросмотренные уведомления.

   Откроется окно со списком уведомлений. По умолчанию выбрана вкладка **Все уведомления** и отображаются уведомления, сгруппированные по уровням важности: *Критические уведомления*, *Предупреждающие уведомления* и *Информационные уведомления*.

2. Выберите вкладку **Система**.

   Отображается список уведомлений с уровнями важности *Критические уведомления* () и *Предупреждающие уведомления* (). Список уведомление включает следующее:

   - Цветной индикатор. Критические уведомления отмечены красным. Предупреждающие уведомления отмечены желтым.

   - Значок, относящийся к теме уведомления: развертывание (), защита (), обновления(), управление устройствами (), Защита от эксплойтов (), Сервер администрирования ().

   - Описание уведомления.

   - Значок флажка. Серый флаг используется для уведомлений, которым присвоен статус *Не просмотрено*. Когда вы выбираете серый флаг и назначаете статус *Просмотрено* для уведомления, цвет флажка изменится на белый.

- Ссылка на рекомендуемое действие. Когда вы выполняете рекомендуемое действие, переходя по ссылке, уведомлению присваивается статус *Просмотрено*.
- Количество дней, прошедших с даты регистрации уведомления на Сервере администрирования.

3. Выберите вкладку **Больше**.

   Отображается список уведомлений с уровнем важности *Информационное уведомление*.

   Структура списка такая же, как и для списка на вкладке **Система** (описание приведено выше). Отличается только отсутствием цветного индикатора.

Вы можете фильтровать уведомления по датам, когда они были зарегистрированы на Сервере администрирования. Используйте флажок **Показать фильтр**, чтобы настроить фильтр.

Чтобы просмотреть экранные уведомления на виджете:

1. В разделе **Панель мониторинга** выберите **Добавить или восстановить веб-виджет**.
2. В открывшемся окне нажмите на категорию **Другие**, выберите виджет **Уведомления, выбранные по уровню важности** и нажмите на кнопку Добавить.

   Виджет отображается на вкладке **Панель мониторинга**. По умолчанию на виджете отображаются уведомления с уровнем важности *Критическое*.

   Вы можете нажать на кнопку **Параметры** на виджете и изменить параметры виджета, чтобы просмотреть уведомления с уровнем важности *Предупреждающие уведомления*. Или вы можете добавить другой виджет: **Уведомления, выбранные по уровню важности** с уровнем важности *Предупреждающие уведомления*.

   Список уведомлений на виджете ограничен размером и включает только два уведомления. Эти два уведомления относятся к последним событиям.

Список уведомлений виджета включает следующее:

- Значок, относящийся к теме уведомления: развертывание, защита, обновления, управление устройствами, Защита от эксплойтов, Сервер администрирования.
- Описание уведомления со ссылкой на рекомендуемое действие. Когда вы выполняете рекомендуемое действие, переходя по ссылке, уведомлению присваивается статус *Просмотрено*.
- Количество дней или часов, прошедших с даты регистрации уведомления на Сервере администрирования.
- Ссылка на другие уведомления. Перейдите по ссылке к просмотру уведомлений в разделе **Уведомления** в разделе **Мониторинг и отчеты**.

О статусах устройства

Kaspersky Security Center присваивает статус каждому управляемому устройству. Конкретный статус зависит от того, выполнены ли условия, определенные пользователем. В некоторых случаях при присваивании статуса устройству Kaspersky Security Center учитывает видимость устройства в сети (см. таблицу ниже). Например, если управляемому устройству был присвоен статус *Критический*, так как выполнено условие *Базы устарели*, а затем для устройства стало видимо в сети, то устройству присваивается статус *OK*. Если Kaspersky Security Center не находит устройство в сети в течение двух часов, видимость устройства принимает значение *Не в сети*.

Существуют следующие статусы:

- *Критический* или *Критический / Видим в сети*.
- *Предупреждение* или *Предупреждение / Видим в сети*.
- *ОК* или *ОК / Видим в сети*.

В таблице ниже приведены условия по умолчанию для присвоения устройству статуса *Критический* или *Предупреждение* и их возможные значения.

Условия присвоения статусов устройству

Условие	Описание условия	Доступные значения
Приложение безопасности не установлено	Агент администрирования установлен на устройстве, но не установлено приложение безопасности.	• Переключатель включен. • Переключатель выключен.
Обнаружено много вирусов	В результате работы задач поиска вирусов, например, задачи *Поиск вредоносного ПО*, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение.	Более 0.
Уровень постоянной защиты отличается от уровня, установленного администратором	Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства.	• Остановлена. • Приостановлена. • Выполняется.
Давно не выполнялся поиск вредоносного ПО	Устройство видимо в сети и на устройстве установлено приложение безопасности, но ни задача *Поиск вредоносного ПО*, ни задача локальной проверки не выполнялись больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее.	Более 1 дня.
Базы устарели	Устройство видимо в сети и на устройстве установлено приложение безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее.	Более 1 дня.
Давно не подключались	Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено.	Более 1 дня.
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. Управляемые устройства могут иметь статус, определяемый управляемыми приложениями, независимо от параметров Kaspersky Security Center. После того как этот статус вернет один из статусов, определенных Kaspersky Security Center, Сервер администрирования Kaspersky Security Center присваивает управляемому устройству предельный статус из тех, которые были возвращены управляемым приложением и присвоены Сервером администрирования Kaspersky Security Center. Статусы устройств определенные приложениями имеют описания, переданные управляемыми приложениями. Вы можете просмотреть описания в списке управляемых устройств в столбце **Описание статуса**.	• Переключатель выключен. • Переключатель включен.
На устройстве заканчивается дисковое пространство	Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы *Критический* или *Предупреждение* меняются на статус *OK*, когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению.	Более чем 0 МБ.
Устройство стало неуправляемым	Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования.	• Переключатель выключен. • Переключатель включен.
Защита выключена	Устройство видимо в сети, но приложение безопасности на устройстве отключено больше указанного времени. В этом случае состояние приложения безопасности *Остановлено* или *Сбой* и отличается от следующих: *Запускается*, *Выполняется* или *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 позволяет настроить автоматическое переключение статуса устройства в группе администрирования при выполнении заданных условий. При выполнении заданных условий клиентскому устройству присваивается один из статусов: *Критический* или *Предупреждение*. При невыполнении заданных условий клиентскому устройству присваивается статус *OK*.

Разным значениям одного условия могут соответствовать разные статусы. Например, по умолчанию при соблюдении условия **Базы устарели** со значением **Более 3 дней** клиентскому устройству присваивается статус *Предупреждение*, а со значением **Более 7 дней** – статус *Критический*.

Если вы обновляете Kaspersky Security Center с предыдущей версии, значение условия **Базы устарели** для назначения статуса *Критический* или *Предупреждение* не изменится.

Настройка переключения статусов устройств

Вы можете изменить условия присвоения статусов *Критический* или *Предупреждение* устройству.

Чтобы изменить статус устройства на Критический:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Иерархия групп**.
2. В открывшемся списке групп перейдите по ссылке с названием группы, для которой вы хотите изменить переключение статусов устройств.
3. В 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 **Активы (Устройства)** → **Иерархия групп**.
2. В открывшемся списке групп перейдите по ссылке с названием группы, для которой вы хотите изменить переключение статусов устройств.
3. В 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*.

Настройка параметров доставки уведомлений

Вы можете настроить уведомления о событиях, возникающих в Kaspersky Security Center. В зависимости от выбранного способа уведомления доступны следующие типы уведомлений:

- Электронная почта – при возникновении события приложение Kaspersky Security Center посылает уведомление на указанные адреса электронной почты.
- SMS – при возникновении события приложение Kaspersky Security Center посылает уведомления на указанные номера телефонов.
- Исполняемый файл – при возникновении события исполняемый файл запускается на Сервере администрирования.

Чтобы настроить параметры доставки уведомлений о событиях, возникших в Kaspersky Security Center:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Перейдите в раздел **Уведомление** и в правой панели выберите вкладку с требуемым способом уведомления:

   - **Электронная почта**

     На вкладке **Электронная почта** можно настроить уведомления о событиях по электронной почте.

     В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой.

     В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

     - IPv4-адрес или IPv6-адрес;
     - Имя устройства в сети Windows (NetBIOS-имя);
     - DNS-имя SMTP-сервера.

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Если вы включите параметр **Использовать DNS и MX поиск**, вы сможете использовать несколько MX-записей IP-адреса для одного и того же DNS-имени SMTP-сервера. Одно DNS-имя может иметь несколько MX-записей с различными приоритетами полученных электронных писем. Сервер администрирования пытается отправлять уведомления по электронной почте на SMTP-сервер в порядке возрастания приоритета MX-записей.

Если вы включили параметр **Использовать DNS и MX поиск** и не разрешили использование параметров TLS, рекомендуется использовать параметры DNSSEC на вашем серверном устройстве в качестве дополнительной меры защиты при отправке уведомлений по электронной почте.

Если параметр **Использовать ESMTP-аутентификацию** включен, вы можете указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию параметр не выбран и параметры ESMTP-аутентификации недоступны.

Вы можете указать параметры подключения TLS для SMTP-сервера:

- **Не использовать TLS**

Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

- **Использовать TLS, если поддерживается SMTP-сервером**

Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.

- **Всегда использовать TLS, для проверки срока действия сертификата сервера**

Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы выбрали значение **Всегда использовать TLS, для проверки срока действия сертификата сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

Вы можете указать сертификат для TLS подключения, перейдя по ссылке **Задать сертификаты**:

- Выберите файл сертификата SMTP-сервера:

Вы можете получить файл со списком сертификатов от доверенного центра сертификации и загрузить его на Сервер администрирования. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также доверенным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от доверенного центра сертификации.

- Выберите файл сертификата клиента:

Вы можете использовать сертификат, полученный из любого источника, например, от любого доверенного центра сертификации. Вам нужно указать сертификат и его закрытый ключ, используя один из следующих типов сертификатов:

- Сертификат X-509:

Вам нужно указать файл с сертификатом и файл с закрытым ключом. Оба файла не зависят друг от друга. Порядок загрузки файлов не имеет значения. Когда оба файла загружены, необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

- Контейнер pkcs12:

Вам нужно загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

В поле **Тема** укажите тему электронной почты. Вы можете оставить поле пустым.

В раскрывающемся списке **Тема шаблона** выберите шаблон для темы вашего электронного письма. Переменная, в соответствии с выбранным шаблоном, автоматически отображается в поле **Тема**. Вы можете создать тему электронной почты, выбрав несколько шаблонов темы.

В окне **Адрес электронной почты отправителя** укажите адрес отправителя электронной почты. Если вы оставите поле пустым, по умолчанию используется адрес получателя. Не рекомендуется использовать несуществующий адрес.

В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый приложением при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив подстановочные параметры с подробными данными события.

> Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

По нажатию на кнопку **Отправить тестовое сообщение** можно проверить, правильно ли настроены сообщения: приложение отправляет тестовые сообщения на указанные адреса электронной почты.

- **SMS**

На вкладке **SMS** можно настроить отправку SMS-уведомлений о различных событиях на мобильный телефон. SMS-сообщения отправляются через почтовый шлюз.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес;
- Имя устройства в сети Windows (NetBIOS-имя);
- DNS-имя SMTP-сервера.

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Если параметр **Использовать ESMTP-аутентификацию** включен, вы можете указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию параметр не выбран и параметры ESMTP-аутентификации недоступны.

Вы можете указать параметры подключения TLS для SMTP-сервера:

- **Не использовать TLS**

Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

- **Использовать TLS, если поддерживается SMTP-сервером**

Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.

- **Всегда использовать TLS, для проверки срока действия сертификата сервера**

Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы выбрали значение **Всегда использовать TLS, для проверки срока действия сертификата сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

Вы можете указать файл сертификата SMTP-сервера, перейдя по ссылке **Задать сертификаты**:

Вы можете получить файл со списком сертификатов от доверенного центра сертификации и загрузить его на Сервер администрирования. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также доверенным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от доверенного центра сертификации.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой. Уведомления доставляются на телефоны, номера которых связаны с указанными адресами электронной почты.

В поле **Тема** укажите тему электронной почты.

В раскрывающемся списке **Тема шаблона** выберите шаблон для темы вашего электронного письма. Переменная, в соответствии с выбранным шаблоном, отображается в поле **Тема**. Вы можете создать тему электронной почты, выбрав несколько шаблонов темы.

В окне **Адрес электронной почты отправителя: если параметр не задан, будет использоваться адрес получателя. Внимание: не рекомендуется указывать в этом поле несуществующий адрес электронной почты** укажите адрес отправителя электронной почты. Если вы оставите поле пустым, по умолчанию используется адрес получателя. Не рекомендуется использовать несуществующий адрес.

В поле **Номера телефонов получателей SMS-сообщений** укажите номера мобильных телефонов для получения SMS.

В поле **Текст уведомления** напишите текст уведомления о событии, отправляемый приложением при возникновении события. Текст может содержать подстановочные параметры, такие как имя события, имя устройства и имя домена.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

Нажмите на кнопку **Отправить тестовое сообщение**, чтобы проверить правильно ли настроены сообщения: приложение отправляет тестовые сообщения указанным получателям.

- **Исполняемый файл для запуска**

  Если выбран этот способ уведомления, в поле ввода можно указать, какое приложение будет запущено при возникновении события.

  В поле **Исполняемый файл, который запустится на Сервере администрирования при возникновении события** укажите папку и имя файла, который запустится. Перед указанием файла подготовьте файл и укажите подстановочные параметры, которые определяют сведения о событии, которые будут отправлены в сообщении. Указанные папка и файл должны находиться на Сервере администрирования.

  При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

3. На вкладке настройте параметры уведомлений.

4. Нажмите на кнопку **OK**, чтобы закрыть окно свойств Сервера администрирования.

Сохраненные параметры доставки уведомлений применяются ко всем событиям, которые возникают в Kaspersky Security Center.

Можно изменить значения параметров доставки уведомлений для определенных событий в разделе **Настройка событий** в параметрах Сервера администрирования, параметрах политики или параметрах приложения.

Уведомление о событиях с помощью исполняемого файла

Kaspersky Security Center позволяет с помощью запуска исполняемого файла уведомлять администратора о событиях на клиентских устройствах. Исполняемый файл должен содержать другой исполняемый файл с подстановочными параметрами события, которые нужно передать администратору (см. таблицу ниже).

Подстановочные параметры для описания события

Подстановочный параметр	Описание подстановочного параметра
%SEVERITY%	Уровень важности события. Возможные значения: • **Информационное сообщение** • **Предупреждение** • **Возникшая ошибка** • **Критическое**
%COMPUTER%	Имя устройства, на котором произошло событие. Максимальная длина имени устройства равна 256 символов.
%DOMAIN%	Имя домена устройства, на котором произошло событие.
%EVENT%	Имя типа события. Максимальная длина названия типа события равна 50 символов.
%DESCR%	Описание события. Максимальная длина описания равна 1000 символов.
%RISE_TIME%	Время создания события.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Название задачи. Максимальная длина названия задачи равна 100 символов.
%KL_PRODUCT%	Название приложения.
%KL_VERSION%	Номер версии приложения.

Подстановочный параметр	Описание подстановочного параметра
%KLCSAK_EVENT_SEVERITY_NUM%	Код уровня важности события. Возможные значения: • 1 – **Информационное сообщение**. • 2 – **Предупреждение**. • 3 – **Сбой**. • 4 – **Критическое**.
%HOST_IP%	IP-адрес устройства, на котором произошло событие.
%HOST_CONN_IP%	IP-адрес соединения устройства, на котором произошло событие.

Пример:
Для уведомления о событии используется исполняемый файл (например, script1.bat), внутри которого запускается другой исполняемый файл (например, script2.bat) с подстановочным параметром %COMPUTER%. При возникновении события на устройстве администратора будет запущен файл script1.bat, который, в свою очередь, запустит файл script2.bat с параметром %COMPUTER%. В результате администратор получит имя устройства, на котором произошло событие.

Объявления "Лаборатории Касперского"

В этом разделе описано, как использовать, настраивать и отключать объявления "Лаборатории Касперского".

Об объявлениях "Лаборатории Касперского"

Раздел Объявления "Лаборатории Касперского" (**Мониторинг и отчеты → Объявления "Лаборатории Касперского"**) предоставляет информацию о вашей версии Kaspersky Security Center и управляемых приложениях, установленных на управляемых устройствах. Kaspersky Security Center периодически обновляет информацию в разделе, удаляет устаревшие объявления и добавляет новую информацию.

Kaspersky Security Center показывает только те объявления "Лаборатории Касперского", которые относятся к текущему подключенному Серверу администрирования и приложениям "Лаборатории Касперского", установленным на управляемых устройствах этого Сервера администрирования. Объявления отображаются индивидуально для любого типа Сервера администрирования – главного, подчиненного или виртуального.

Для получения объявлений "Лаборатории Касперского" Сервер администрирования должен иметь подключение к интернету.

Объявления включают информацию следующих типов:

- Объявления, связанные с безопасностью.

  Объявления, связанные с безопасностью, предназначены для того, чтобы приложения "Лаборатории Касперского", установленные в вашей сети, были в актуальном состоянии и были полностью функциональными. В объявлениях может содержаться информация о критических обновлениях для приложений "Лаборатории Касперского", исправлениях для обнаруженных уязвимостей и способах устранения других проблем в приложениях "Лаборатории Касперского". Объявления, связанные с безопасностью, включены по умолчанию. Если вы не хотите получать объявления, вы можете отключить эту функцию.

  Чтобы показать вам информацию, которая соответствует вашей конфигурации защиты сети, Kaspersky Security Center отправляет данные на облачные серверы "Лаборатории Касперского" и получает только те объявления, которые относятся к приложениям "Лаборатории Касперского", установленным в вашей сети. Данные, которые могут быть отправлены на серверы, описаны в Лицензионном соглашении, которое вы принимаете при установке Сервера администрирования Kaspersky Security Center.

- Рекламные объявления.

  Рекламные объявления включают информацию о специальных предложениях для ваших приложений "Лаборатории Касперского", рекламу и новости "Лаборатории Касперского". Рекламные объявления по умолчанию выключены. Вы получаете этот тип объявлений только в том случае, если вы включили Kaspersky Security Network (KSN). Вы можете выключить рекламные объявления, выключив KSN.

  Чтобы показывать вам только актуальную информацию, которая может быть полезна для защиты ваших сетевых устройств и выполнения повседневных задач, Kaspersky Security Center отправляет данные на облачные серверы "Лаборатории Касперского" и получает соответствующие объявления. Данные, которые могут быть отправлены на серверы, описан в разделе "Обрабатываемые данные" Положения о KSN.

Информация разделена на следующие категории по важности:

1. Критическая информация.
2. Важная новость.
3. Предупреждение.
4. Информационное сообщение.

При появлении новой информации в разделе Объявления "Лаборатории Касперского" Kaspersky Security Center Web Console отображает метку уведомления, соответствующую уровню важности объявлений. Вы можете нажать на метку, чтобы просмотреть это объявление в разделе Объявления "Лаборатории Касперского".

Вы можете указать параметры объявлений "Лаборатории Касперского", включая категории объявлений, которые вы хотите просматривать, и место отображения метки уведомления.

Настройка параметров объявлений "Лаборатории Касперского"

В разделе Объявления "Лаборатории Касперского" вы можете указать параметры объявлений "Лаборатории Касперского", включая категории объявлений, которые вы хотите просматривать, и где отображать метку уведомления.

Чтобы настроить объявления "Лаборатории Касперского":

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Объявления "Лаборатории Касперского"**.
2. Перейдите по ссылке **Параметры**.

   Откроется окно объявлений "Лаборатории Касперского".
3. Задайте следующие параметры:

   - Выберите уровень важности объявлений, которые вы хотите просматривать. Объявления других категорий отображаться не будут.
   - Выберите расположение, где вы хотите видеть метку уведомления. Метка может отображаться во всех разделах консоли или в разделе **Мониторинг и отчеты** и его подразделах.
4. Нажмите на кнопку **OK**.

   Параметры объявлений "Лаборатории Касперского" настроены.

Выключение объявлений "Лаборатории Касперского"

Раздел объявлений "Лаборатории Касперского" (**Мониторинг и отчеты → Объявления "Лаборатории Касперского"**) предоставляет информацию о вашей версии Kaspersky Security Center и управляемых приложениях, установленных на управляемых устройствах. Если вы не хотите получать объявления "Лаборатории Касперского", вы можете отключить эту функцию.

Объявления "Лаборатории Касперского" включают в себя информацию двух типов: объявления, связанные с безопасностью, и рекламные объявления. Вы можете выключить объявления каждого типа отдельно.

Чтобы выключить объявления, связанные с безопасностью:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Объявления "Лаборатории Касперского"**.

3. Переведите переключатель в положение **Объявления безопасности Выключены**.

4. Нажмите на кнопку **Сохранить**.

   Объявления "Лаборатории Касперского" выключены.

Рекламные объявления по умолчанию выключены. Вы получаете рекламные сообщения только в том случае, если вы включили Kaspersky Security Network (KSN). Вы можете выключить этот тип объявлений, отключив KSN.

Чтобы отключить объявления:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.

3. Выключите параметр **Использовать Kaspersky Security Network Включено**.

4. Нажмите на кнопку **Сохранить**.

   Объявления выключены.

Просмотр информации об обнаруженных угрозах

Вы можете включить или отключить отображение информации об алертах.

*Чтобы включить или выключить отображение раздела **Алерты** в главном меню:*

1. В главном меню перейдите в параметры своей учетной записи и выберите **Параметры интерфейса.**
2. В появившемся окне **Параметры интерфейса** включите или выключите параметр **Показать EDR-алерты**.
3. Нажмите на кнопку **Сохранить**.

В консоли отображается раздел **Алерты** в разделе **Мониторинг и отчеты** главного меню. В разделе **Алерты** вы можете просматривать информацию об обнаруженных угрозах на устройствах. Если вы добавите лицензионный ключ для EDR Optimum, Kaspersky Security Center Web Console автоматически отобразит подраздел **Алерты** в разделе **Мониторинг и отчеты** главного меню. Также вы можете добавить виджет, в котором отображается информация об алертах.

Подраздел **Алерты** отображается автоматически, только если вы добавили лицензионный ключ для EDR Optimum перед включением параметра **Показать EDR-алерты**. Если вы добавили лицензионный ключ после включения параметра **Показать EDR-алерты**, подраздел **Алерты** будет отображаться только после повторного включения этого параметра.

Для корректного отображения подробной информации об обнаруженных угрозах в карточке алерта вам необходимо установить плагин Kaspersky Endpoint Agent и совместимую версию плагина Kaspersky Endpoint Security (Kaspersky Endpoint Security для Linux 12.1 или выше, Kaspersky Endpoint Security для Mac 12.1 или выше, Kaspersky Endpoint Security для Windows 12.6 или выше).

Используйте меню **Фильтр**, чтобы отфильтровать алерты по дате и значениям поля.

Поле **Тип объекта** содержит одно из следующих значений:

- Нет данных
- Фишинговая ссылка
- Вирус
- Троянское приложение
- Вредоносная утилита
- Троянское приложение удаленного администрирования
- Червь
- Другое приложение
- Рекламное приложение
- Порнографическое приложение
- Опасно упакованное приложение
- Опасное поведение

Поле **Автоматический ответ** содержит одно из следующих значений:

- Обнаружен вредоносный объект
- Объект удален
- Объект вылечен
- Не удалось вылечить объект
- Объект помещен на карантин
- Обнаружен архив, защищенный паролем
- Обнаружен вирус

Cloud Discovery

Kaspersky Security Center позволяет отслеживать использование облачных сервисов на управляемых устройствах с операционной системой Windows и блокировать доступ к нежелательным облачным сервисам. Cloud Discovery отслеживает попытки пользователей получить доступ к этим службам через браузеры и настольные приложения. Также отслеживает попытки доступа пользователей к облачным сервисам через незашифрованные соединения (например, по протоколу HTTP). Эта функция позволяет выявлять и прекращать скрытое несанкционированное использование облачных сервисов.

Возможность блокировки доступна только в том случае, если вы активировали Kaspersky Security Center по лицензии Kaspersky Next EDR Optimum или Kaspersky Symphony XDR.

Возможность блокировки доступна только при использовании Kaspersky Endpoint Security 11.2 для Windows и выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.

Можно включить функцию Cloud Discovery и выбрать политики безопасности или профили, для которых ее требуется включить. Можно также включать и выключать функцию отдельно для каждой политики безопасности или профиля. Вы можете заблокировать доступ к облачным сервисам, к которым вы хотите ограничить доступ для пользователей.

Чтобы заблокировать доступ к нежелательным облачным сервисам, убедитесь, что выполнены следующие условия:

- Вы используете версию Kaspersky Endpoint Security 11.2 для Windows или выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.
- Вы приобрели лицензию на Kaspersky, которая дает возможность блокировать доступ к нежелательным облачным сервисам. Подробную информацию см. в справке Kaspersky.

Информация об удачных и заблокированных попытках доступа к облачным сервисам отображается в виджете Cloud Discovery и в отчетах Cloud Discovery. Виджет также показывает уровень риска каждого облачного сервиса. Kaspersky Security Center получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных профилями безопасности, в которых они включены.

Включение функции Cloud Discovery с помощью виджета

Функция Cloud Discovery получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных политиками безопасности, в которых она включена. Включить или выключить Cloud Discovery можно только для политики Kaspersky Endpoint Security для Windows.

Существуют два способа включить функцию Cloud Discovery:

- С помощью виджета Cloud Discovery.
- В свойствах политики Kaspersky Endpoint Security для Windows.

  Подробную информацию о том, как включить функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security для Windows, см. в разделе Cloud Discovery справки Kaspersky Endpoint Security для Windows.

Обратите внимание, что вы можете выключить функцию Cloud Discovery только в параметрах политики Kaspersky Endpoint Security для Windows.

Чтобы включить Cloud Discovery, у вас должно быть право **Запись** в функциональной области **Общие функции: Базовая функциональность**.

Чтобы включить функцию Cloud Discovery с помощью виджета Cloud Discovery:

1. Откройте Kaspersky Security Center.
2. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
3. В виджете **Cloud Discovery** нажмите на кнопку **Включить**.

   Если у вас установлен Kaspersky Endpoint Security для Windows версии 12.4, включите функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security для Windows. Подробнее см. раздел Cloud Discovery справки Kaspersky Endpoint Security для Windows.

   Если у вас версия Kaspersky Endpoint Security для Windows ниже версии 12.4, обновите плагин Kaspersky Endpoint Security для Windows до версии 12.5.

4. В открывшемся окне **Включить Cloud Discovery** выберите политики безопасности, для которых вы хотите включить функцию и нажмите на кнопку **Включить**.

   Следующие параметры политики будут включены автоматически: **Внедрение скрипта в веб-трафик для взаимодействия с веб-страницами**, **Мониторинг веб-сеансов** и **Проверка зашифрованных подключений**.

Функция Cloud Discovery включена, виджет добавлен в панель мониторинга.

Добавление виджета Cloud Discovery в панель мониторинга

Вы можете добавить виджет **Cloud Discovery** в панель мониторинга, чтобы отслеживать использование облачных сервисов на управляемых устройствах.

Чтобы добавить виджет Cloud Discovery в панель мониторинга, у вас должно быть право **Запись** в функциональной области **Общие функции: Базовая функциональность**.

Чтобы добавить виджет Cloud Discovery в панель мониторинга:

1. Откройте Kaspersky Security Center.
2. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
3. Нажмите на кнопку **Добавить или восстановить веб-виджет**.
4. В списке доступных виджетов нажмите на значок шеврона (>) рядом с категорией **Другое**.
5. Выберите виджет **Cloud Discovery** и нажмите на кнопку **Добавить**.

   Если функция Cloud Discovery выключена, следуйте инструкциям в разделе Включение функции Cloud Discovery с помощью виджета.

Выбранный виджет будет добавлен в конец панели мониторинга.

Просмотр информации об использовании облачных сервисов

Виджет **Cloud Discovery** показывает информацию о попытках доступа к облачным сервисам. Виджет также показывает уровень риска каждого облачного сервиса. Kaspersky Security Center получает информацию об использовании облачных сервисов со всех управляемых устройств, защищенных только теми профилями безопасности, в которых включена эта функция.

Перед просмотром убедитесь, что:

- Виджет Cloud Discovery добавлен в панель мониторинга.
- Функция Cloud Discovery включена.
- У вас есть право **Чтение** в функциональной области **Общие функции: Базовая функциональность**.

Чтобы посмотреть виджет Cloud Discovery:

1. Откройте Kaspersky Security Center.
2. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **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 и отчеты** → **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 по лицензии Kaspersky Next EDR Optimum или Kaspersky Symphony XDR.
Возможность блокировки доступна только при использовании Kaspersky Endpoint Security 11.2 для Windows и выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.

Уровень риска облачных сервисов

Cloud Discovery определяет уровень риска для каждого облачного сервиса. Уровень риска помогает определить сервисы, не соответствующие требованиям безопасности вашей организации. Например, вы можете принять во внимание уровень риска при принятии решения о блокировке доступа к определенному сервису.

Уровень риска является оценочным показателем и ничего не говорит о качестве облачного сервиса или о производителе. Уровень риска – это рекомендация экспертов "Лаборатории Касперского".

Уровни риска облачных сервисов отображаются в виджете Cloud Discovery и в списке всех контролируемых облачных сервисов.

Блокировка доступа к нежелательным облачным сервисам

Вы можете заблокировать доступ к облачным сервисам, к которым вы хотите ограничить доступ для пользователей. Вы также можете разрешить доступ к облачным сервисам, которые ранее были заблокированы.

Например, уровень риска можно учесть при принятии решения о блокировке доступа к определенному сервису.

Вы можете заблокировать или разрешить доступ к облачным сервисам для политики безопасности или профиля политики.

Существует два способа заблокировать доступ к нежелательным облачным сервисам:

- С помощью виджета Cloud Discovery.

  В этом случае вы можете заблокировать доступ к сервисам по очереди.

- В свойствах политики Kaspersky Endpoint Security для Windows.

  В этом случае вы можете заблокировать доступ к сервисам по очереди или сразу всю категорию.

  Подробную информацию о том, как включить функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security для Windows, см. в разделе Cloud Discovery справки Kaspersky Endpoint Security для Windows.

Чтобы заблокировать или разрешить доступ к облачному сервису с помощью виджета:

1. Откройте виджет Cloud Discovery и выберите требуемый облачный сервис.
2. В панели **Топ-10 устройств, использующих эту службу** найдите политику безопасности или профиль политики, для которых вы хотите заблокировать или разрешить службу.
3. В соответствующей строке в столбце **Статус доступа в политике или профиле политики** выполните одно из следующих действий:
   - Чтобы заблокировать службу, в раскрывающемся списке выберите **Заблокировано**.
   - Чтобы разрешить службу, в раскрывающемся списке выберите **Разрешено**.
4. Нажмите на кнопку **Сохранить**.

Доступ к выбранной службе заблокирован или разрешен для политики безопасности или профиля политики.

Журнал активности Kaspersky Security Center Web Console

Журнал активности Kaspersky Security Center Web Console может помочь выяснить причины сбоя программного обеспечения. Когда вы обращаетесь в Службу технической поддержки "Лаборатории Касперского" в случае сбоя Kaspersky Security Center Web Console, специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить от вас файлы журнала Kaspersky Security Center Web Console. Файлы журнала событий Kaspersky Security Center Web Console хранятся в папке <Папка установки Kaspersky Security Center Web Console>/logs все время использования приложения. Файлы журнала не отправляются автоматически специалистам Службы технической поддержки "Лаборатории Касперского".

Чтобы включить журнал активности Kaspersky Security Center Web Console,

установите флажок **Включить запись в журнал Kaspersky Security Center Web Console** в окне **Параметры подключения Kaspersky Security Center Web Console** мастера установки Kaspersky Security Center Web Console.

Файлы журнала записываются в текстовом формате.

Имена файлов журнала записываются в формате -<имя компонента>.<имя устройства>-<номер ревизии файла>.ГГГГ-ММ-ДД, где:

- <имя компонента> – имя компонента Kaspersky Security Center или имя плагина управления Kaspersky Security Center Web Console.
- <имя устройства> – имя устройства, на котором запущен компонент или плагин (<имя компонента>).
- <номер ревизии файла> – номер файла журнала, созданного для компонента или плагина <имя компонента>, который запущен на устройстве <имя устройства>. В течение одного дня можно создать несколько файлов журнала для одного и того же компонента или плагина (<имя компонента>) и устройства (<имя устройства>). Максимальный размер файла журнала составляет 50 МБ. При достижении максимального размера файла создается новый файл журнала. Новый файл журнала (<номер ревизии файла>) увеличивается на 1.
- ГГГГ, ММ, и ДД это год, месяц и день, когда была создана первая запись журнала. Новый файл журнала создается, когда начинается новый день.

Интеграция Kaspersky Security Center с другими решениями

В этом разделе описывается, как настроить доступ из Kaspersky Security Center Web Console к другому приложению "Лаборатории Касперского", например Kaspersky Managed Detection and Response. В этом разделе также описано как настроить экспорт в SIEM-системы.

Установка фонового соединения

Чтобы приложение Kaspersky Security Center Web Console могло выполнять свои фоновые задачи, необходимо установить фоновое соединение между Kaspersky Security Center Web Console и Сервером администрирования. Вы можете установить это соединение, только если в вашей учетной записи есть право **Изменение списков управления доступом объектов** в функциональной области **Общие функции: Права пользователей**.

Если вы устанавливаете плагин Kaspersky Endpoint Security для Windows 12.6 или обновляете плагин Kaspersky Endpoint Security для Windows с версии ниже 11.7 и фоновое соединение еще не установлено, отображается уведомление о том, что необходимо установить фоновое соединение. Также вам нужно будет предоставить учетной записи службы права **Общие функции: Операции с Сервером администрирования**.

Чтобы установить фоновое соединение:

1. В главном меню перейдите в раздел **Параметры** → **Интеграция**.
2. В разделе **Интеграция** переключите переключатель установки фонового соединения в положение: **Фоновое соединение для интеграции Включено**.
3. В разделе **Включить фоновое соединение** нажмите на кнопку **ОК**.

Фоновое соединение между Kaspersky Security Center Web Console и Сервером администрирования установлено. Сервер администрирования создает учетную запись для фонового подключения, и эта учетная запись используется как служебная учетная запись для поддержания взаимодействия Kaspersky Security Center с другим приложением или решением "Лаборатории Касперского". Имя этой учетной записи службы содержит префикс NWCSvcUser.

Сервер администрирования автоматически меняет пароль учетной записи службы каждые 30 дней в целях безопасности. Вы не можете удалить учетную запись службы вручную. Сервер администрирования автоматически удаляет эту учетную запись при отключении межсервисного соединения. Сервер администрирования создает единую учетную запись службы для каждой Консоли администрирования и назначает все учетные записи службы группе безопасности с именем ServiceNwcGroup. Сервер администрирования создает эту группу безопасности автоматически в процессе установки Kaspersky Security Center. Вы не можете удалить эту группу безопасности вручную.

Экспорт событий в SIEM-системы

В этом разделе описывается, как настроить экспорт событий в SIEM-системы.

Настройка экспорта событий в SIEM-системы

Kaspersky Security Center позволяет выполнять настройку одним из способов: экспорт в любую SIEM-систему, использующую формат Syslog, экспорт в QRadar, Splunk, ArcSight SIEM-системы, использующие форматы LEEF и CEF, или экспорт событий в SIEM-системы прямо из базы Kaspersky Security Center. По завершении этого сценария Сервер администрирования автоматически отправляет события в SIEM-систему.

Предварительные требования

Перед началом настройки экспорта событий в Kaspersky Security Center:

- Узнайте больше о методах экспорта событий.
- Убедитесь, что у вас есть значения системных параметров.

> Вы можете выполнять шаги этого сценария в любом порядке.

Процесс экспорта событий в SIEM-систему состоит из следующих шагов:

- **Настройка SIEM-системы для получения событий из Kaspersky Security Center**

  Инструкции: Настройка экспорта событий в SIEM-системе.

- **Выбор события, которые вы хотите экспортировать в SIEM-систему:**

Инструкции:

- Консоль администрирования: Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog, Выбор общих событий для экспорта в формате Syslog.
- Kaspersky Security Center Web Console: Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog, Выбор общих событий для экспорта в формате Syslog.

- **Настройка экспорта событий в SIEM-систему одним из следующих способов:**
  - Использование протоколов TCP, UDP или TLS over TCP.

    Инструкции:

    - Консоль администрирования: Настройка экспорта событий в SIEM-системы.
    - Kaspersky Security Center Web Console: Настройка экспорта событий в SIEM-системы.
  - Использование экспорта событий напрямую из базы данных Kaspersky Security Center. В базе данных Kaspersky Security Center представлен набор публичных представлений; вы можете найти описание этих общедоступных представлений в документе klakdb.chm.

Результаты

После настройки экспорта событий в SIEM-систему вы можете просматривать результаты экспорта, если вы выбрали события, которые хотите экспортировать.

Предварительные условия

При настройке автоматического экспорта событий в Kaspersky Security Center необходимо указать некоторые параметры SIEM-системы. Рекомендуется уточнить эти параметры заранее, чтобы подготовиться к настройке Kaspersky Security Center.

Для настройки автоматического экспорта событий в SIEM-систему необходимо знать значения следующих параметров:

- **Адрес сервера SIEM-системы**

  Адрес сервера, на котором установлена используемая SIEM-система. Это значение необходимо уточнить в настройках SIEM-системы.

- **Порт сервера SIEM-системы**

  Номер порта, по которому будет установлено соединение между Kaspersky Security Center и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

- **Протокол**

  Протокол, используемый для передачи сообщений из Kaspersky Security Center в SIEM-систему. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

О событиях в Kaspersky Security Center

Kaspersky Security Center позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования. 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 администрирования.

Типы событий

В Kaspersky Security Center существуют следующие типы уведомлений:

- Общие события. Эти события возникают во всех управляемых приложениях "Лаборатории Касперского". Например, общее событие Вирусная атака. Общие события имеют строго определенные синтаксис и семантику. Общие события используются, например, в отчетах и панели мониторинга.
- Специфические события управляемых приложений "Лаборатории Касперского". Каждое управляемое приложение "Лаборатории Касперского" имеет собственный набор событий.

Источники событий

События могут генерироваться следующими приложениями:

- Компоненты приложения Kaspersky Security Center:
  - Сервер администрирования
  - Агент администрирования
  - Сервер iOS MDM
- Управляемые приложения "Лаборатории Касперского"

  Подробнее о событиях, генерируемых управляемыми приложениями "Лаборатории Касперского", см. в документации соответствующего приложения.

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.

Уровень важности события

Каждое событие имеет собственный уровень важности. В зависимости от условий возникновения, событию могут быть присвоены различные уровни важности. Существует четыре уровня важности событий:

- *Критическое событие* – событие, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.
- *Отказ функционирования* – событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы приложения или выполнения процедуры.
- *Предупреждение* – событие, не обязательно являющееся серьезным, однако указывающее на возможное возникновение проблемы в будущем. Чаще всего события относятся к Предупреждениям, если после их возникновения работа приложения может быть восстановлена без потери данных или функциональных возможностей.
- *Информационное сообщение* – событие, возникающее с целью информирования об успешном выполнении операции, корректной работе приложения или завершении процедуры.

Для каждого события задано время хранения, которое можно посмотреть или изменить в Kaspersky Security Center. Некоторые события не сохраняются в базе данных Сервера администрирования по умолчанию, поскольку для них установленное время хранения равно нулю. Во внешние системы можно экспортировать только те события, которые хранятся в базе данных Сервера администрирования не менее одного дня.

Об экспорте событий

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 во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center и получатель событий – SIEM-система. Для успешного экспорта событий необходимо выполнить настройки и в используемой SIEM-системе, и в Kaspersky Security Center. Последовательность настройки не имеет значения: Вы можете либо сначала настроить отправку событий в Kaspersky Security Center, а затем получение событий в SIEM-системе, либо наоборот.

Способы отправки событий из Kaspersky Security Center

Существует три способа отправки событий из Kaspersky Security Center во внешние системы:

- Отправка событий по протоколу Syslog в любую SIEM-систему.

  По протоколу syslog можно передавать любые события, произошедшие на Сервере администрирования Kaspersky Security Center и в приложениях "Лаборатории Касперского", установленных на управляемых устройствах. Протокол Syslog – это стандартный протокол регистрации сообщений. Вы можете использовать этот протокол для экспорта событий в любую SIEM-систему.

  Для этого нужно отметить события, которые вы хотите передать в SIEM-систему. Вы можете отметить события с помощью Консоли администрирования или Kaspersky Security Center Web Console). Только отмеченные события будут передаваться в SIEM-систему. Если вы ничего не отметили, никакие события не будут передаваться.

- Отправка событий по протоколам CEF и LEEF в системы QRadar, Splunk и ArcSight.

  Протоколы CEF и LEEF можно использовать для экспорта общих событий. При экспорте событий по протоколам CEF и LEEF у вас нет возможности выбора определенных экспортируемых событий. Вместо этого выполняется экспорт всех общих событий. Для конвертации событий Kaspersky Security Center в события формата CEF и LEEF используется файл siem_conversion_rules.xml. Этот файл содержит список атрибутов событий Kaspersky Security Center и соответствующие атрибуты событий в формате CEF и LEEF. Также файл siem_conversion_rules.xml содержит правила генерации сообщений, соответствующих событиям. Файл входит в состав комплекта поставки Kaspersky Security Center.

  В отличие от протокола syslog, протоколы CEF и LEEF не являются универсальными. Протоколы CEF и LEEF предназначены для соответствующих SIEM-систем (QRadar, Splunk и ArcSight). Поэтому при выборе экспорта событий по одному из этих протоколов в SIEM-системе используется нужный анализатор.

- Напрямую из базы данных Kaspersky Security Center в любую SIEM-систему.

  Этот способ экспорта событий можно использовать для получения событий напрямую из публичных представлений базы данных с помощью SQL-запросов. Результаты выполнения запроса сохраняются в файл XML, который можно использовать в качестве входных данных для внешней системы. Напрямую из базы данных можно экспортировать только события, доступные в публичных представлениях.

Получение событий SIEM-системой

SIEM-система должна принимать и корректно анализировать события, получаемые из Kaspersky Security Center. Для этого необходимо правильно настроить SIEM-систему. Конфигурация зависит от конкретной используемой SIEM-системы. Однако в конфигурациях всех SIEM-систем существует ряд общих этапов, таких как настройка приемника и анализатора.

О настройке экспорта событий в SIEM-системе

В процедуре экспорта событий из Kaspersky Security Center во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center и получатель событий – SIEM-система. Экспорт событий необходимо настроить в используемой SIEM-системе и в Kaspersky Security Center.

Настройки, выполняемые в SIEM-системе, зависят от того, какую систему вы используете. В общем случае для всех SIEM-систем необходимо настроить приемник сообщений и, при необходимости, анализатор сообщений, для того чтобы разложить полученные сообщения на поля.

Настройка приемника сообщений

Для SIEM-системы необходимо настроить приемник для получения событий, отправляемых Kaspersky Security Center. В общем случае в SIEM-системе необходимо указать следующие параметры:

- **Протокол экспорта или тип входных данных**

  Это протокол передачи сообщений, например UDP. Необходимо указать тот же протокол, который был выбран в Kaspersky Security Center для передачи событий.

- **Порт**

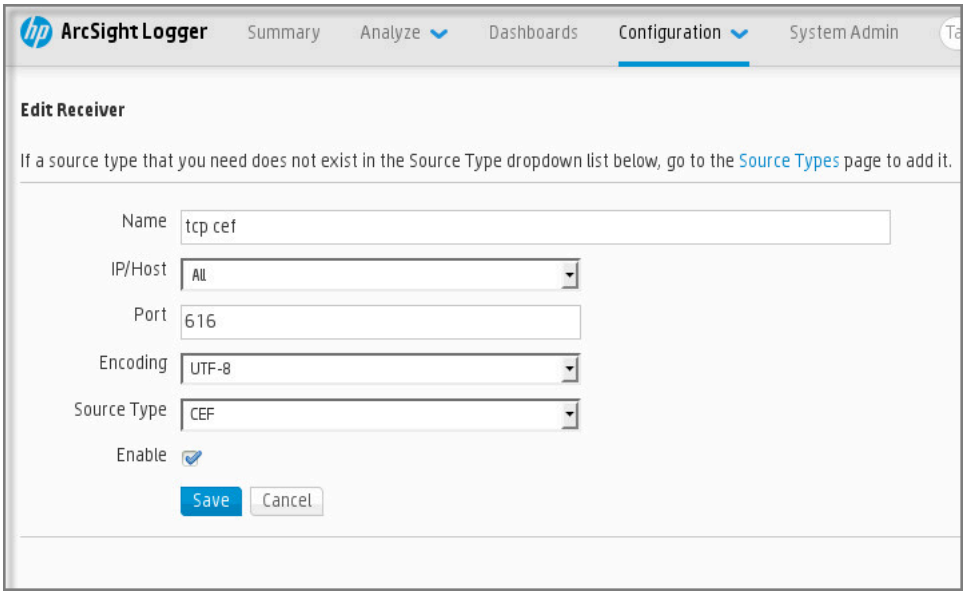
  Номер порта для подключения к Kaspersky Security Center. Необходимо указать тот же номер порта, который был выбран в Kaspersky Security Center для передачи событий.

- **Протокол передачи сообщений или тип исходных данных**

  Протокол, используемый для экспорта событий в SIEM-систему. Это может являться одним из стандартных протоколов: Syslog, CEF или LEEF. SIEM-система выбирает анализатор событий, соответствующий указанному протоколу.

В зависимости от используемой SIEM-системы может потребоваться указать дополнительные параметры приемника сообщений.

На рисунке ниже приведен пример настройки приемника в ArcSight.



Настройка приемника в ArcSight

Анализатор сообщений

Экспортируемые события передаются в SIEM-систему в виде сообщений. Затем к этим сообщениям применяется анализатор, чтобы информация о событиях могла быть использована SIEM-системой. Анализатор сообщений встроен в SIEM-систему; он используется для разбиения содержимого сообщения на соответствующие поля, такие как код события, уровень важности, описание, параметры. В результате SIEM-система имеет возможность выполнять обработку событий, полученных из Kaspersky Security Center, 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.

О выборе событий для экспорта в SIEM-систему в формате syslog

После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться во внешнюю SIEM-систему.

Вы можете настроить экспорт событий в формате Syslog во внешнюю систему на основе одного из следующих условий:

- Выбор общих событий. Если вы выберите экспортируемые события в политике, в свойствах события или в свойствах Сервера администрирования, то в SIEM-систему будут переданы выбранные события, которые произошли во всех приложениях, управляемых данной политикой. Если экспортируемые события были выбраны в политике, вам не удастся их переопределить для отдельного приложения, 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 **Активы (Устройства)** → **Политики и профили политик**.

2. Выберите политику приложения, для которого нужно отметить события.

   Откроется окно свойств политики.

3. Перейдите в раздел **Настройка событий**.
4. Установите флажки рядом с событиями, которые требуется экспортировать в SIEM-систему.
5. Нажмите на кнопку **Отметить для экспорта в SIEM-систему по протоколу Syslog**.

   Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

6. Флажок (✓) появляется в 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 **Активы (Устройства)** → **Управляемые устройства**.

   Отобразится список управляемых устройств.

2. Перейдите по ссылке с названием требуемого устройства в списке управляемых устройств.

   Откроется окно свойств выбранного устройства.

3. 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 меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   - В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**, а затем перейдите по ссылке политики.

2. В открывшемся окне 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 форматах CEF и LEEF

Форматы CEF и LEEF можно использовать для экспорта в SIEM-систему общих событий, а также событий, переданных приложениями "Лаборатории Касперского" Серверу администрирования. Набор экспортируемых событий определен заранее, возможность выбирать экспортируемые события отсутствует. Перед отправкой событий в SIEM-систему (QRadar, ArcSight или Splunk) необходимо интерпретировать события Kaspersky Security Center в события в формате CEF и LEEF, используя правила, указанные в файле siem_conversion_rules.xml.

Формат экспорта можно выбрать в зависимости от того, какую SIEM-систему вы используете. В следующей таблице приведены SIEM-системы и соответствующие им форматы экспорта.

Форматы экспорта событий в SIEM-систему

SIEM-система	Формат экспорта
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) – это специализированный формат событий для IBM Security QRadar SIEM. QRadar может получать, идентифицировать и обрабатывать события, передаваемые по протоколу LEEF. Для протокола LEEF должна использоваться кодировка UTF-8. Более подробную информацию о протоколе LEEF см. на веб-странице IBM Knowledge Center.

- CEF – это стандарт управления типа "открытый журнал", который улучшает совместимость информации системы безопасности от разных сетевых устройств и приложений. Протокол CEF позволяет использовать общий формат журнала событий, чтобы системы управления предприятием могли легко получать и объединять данные для анализа. Для протокола CEF должна использоваться кодировка UTF-8.

При автоматическом экспорте Kaspersky Security Center отправляет общие события в SIEM-систему. Автоматический экспорт событий начинается сразу после включения. В этом разделе описана процедура включения автоматического экспорта событий.

Конвертация событий в формат CEF или LEEF

Перед отправкой событий в SIEM-систему (QRadar, ArcSight или Splunk) необходимо интерпретировать события Kaspersky Security Center в события в формате CEF и LEEF, используя правила, указанные в файле siem_conversion_rules.xml. Этот файл входит в комплект поставки Kaspersky Security Center.

Файл siem_conversion_rules.xml содержит предустановленные правила интерпретации для конвертации событий в формат CEF и LEEF. Если вы хотите использовать дополнительные правила интерпретации событий, вы можете добавить их в файл вручную.

Файл siem_conversion_rules.xml включает следующие секции:

- `<product name="SP_QRADAR" vendor="IBM">`

  Эта секция содержит правила генерации событий в формате LEEF, которые можно экспортировать в SIEM-систему QRadar.

- `<product name="SP_ARCSIGHT" vendor="HP">`.

  Эта секция содержит правила генерации событий в формате CEF, которые можно экспортировать в SIEM-систему ArcSight или Splunk.

В каждом разделе есть подраздел `<common>`, в котором размещены атрибуты событий Kaspersky Security Center и соответствующие им атрибуты событий в формате LEEF. Эти общие атрибуты используются для всех типов событий, которые можно экспортировать.

Каждый раздел также имеет подраздел `<event>`. Каждый подраздел `<event>` содержит дополнительные атрибуты, которые добавляются к атрибутам, указанным в разделе `<common>`.

Вы можете вручную добавить новое правило генерации событий в файл siem_conversion_rules.xml.

Чтобы добавить новое правило генерации событий:

1. Добавьте новый подсекцию `<event>` в секцию `<product name="SP_QRADAR" vendor="IBM">` или `<product name="SP_ARCSIGHT" vendor="HP">`, а затем укажите дополнительные атрибуты события, если необходимо.

2. Если событие состоит только из общих атрибутов, подраздел `<event>` будет пустым.

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Kaspersky Security Center event attributes and corresponding LEEF event attributes --
>
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Generation rule for the GNRL_EV_VIRUS_FOUND event with additional
attributes -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
```

```
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Common Kaspersky Security Center event attributes and corresponding LEEF event attributes --
>
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

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 во внешние системы.

В Kaspersky Security Center можно настроить экспорт событий во внешние системы в формате Syslog.

Процесс экспорта состоит из двух шагов:

1. Включение автоматического экспорта событий. На этом шаге выполняется настройка Kaspersky Security Center таким образом, чтобы выполнялась отправка событий в SIEM-систему. Отправка событий из Kaspersky Security Center начинается сразу после включения автоматического экспорта.

2. Выбор событий, которые будут экспортироваться во внешнюю систему. На этом шаге вам нужно выбрать, какие события будут экспортироваться в SIEM-систему.

Настройка Kaspersky Security Center для экспорта событий в SIEM-систему

Чтобы экспортировать события в SIEM-систему, вам необходимо настроить процесс экспорта из Kaspersky Security Center Web Console.

Перед отправкой событий в SIEM-систему (QRadar, ArcSight или Splunk) необходимо интерпретировать события Kaspersky Security Center в события в формате CEF и LEEF, используя правила, указанные в файле siem_conversion_rules.xml.

Чтобы настроить экспорт в SIEM-системы из Kaspersky Security Center Web Console:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Экспорт в SIEM-систему**.

3. Перейдите по ссылке **Параметры**.

   Откроется раздел **Параметры экспорта**.

4. Укажите параметры в разделе **Параметры экспорта**:

   - **Адрес сервера SIEM-системы**

     Адрес сервера, на котором установлена используемая SIEM-система. Это значение необходимо уточнить в настройках SIEM-системы.

   - **Порт SIEM-системы**

     Номер порта, по которому будет установлено соединение между Kaspersky Security Center и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

   - **Протокол**

     Выберите протокол передачи сообщений в SIEM-систему. Вы можете выбрать протокол TCP, UDP или TLS over TCP.

     Укажите следующие параметры TLS, если вы выбираете TLS over TCP:

     - **Аутентификация Сервера**

       В поле **Аутентификация Сервера** можно выбрать значения **Доверенные сертификаты** или же **Отпечатки SHA**:

       - **Доверенные сертификаты**. Вы можете получить полную цепочку сертификатов (включая корневой сертификат) от доверенного центра сертификации (CA) и загрузить файл в Kaspersky Security Center. Kaspersky Security Center проверяет, подписана ли цепочка сертификатов SIEM-системы также доверенным центром сертификации или нет.

         Чтобы добавить доверенный сертификат, нажмите на кнопку **Выбрать файл центра сертификации** и загрузите сертификат.

       - **Отпечатки SHA**. Вы можете указать отпечатки SHA1 всей цепочки сертификатов SIEM-системы (включая корневой сертификат) в Kaspersky Security Center. Чтобы добавить отпечаток SHA1, введите его в поле **Отпечатки** и нажмите на кнопку **Добавить**.

       С помощью **Добавить проверку подлинности клиента** вы можете сгенерировать сертификат для аутентификации Kaspersky Security Center. Таким образом, вы будете использовать самоподписанный сертификат, выпущенный Kaspersky Security Center. В этом случае для аутентификации сервера SIEM-системы можно использовать как доверенный сертификат, так и отпечаток SHA.

- **Добавить имя субъекта/альтернативное имя субъекта**

  Имя субъекта – это доменное имя, для которого получен сертификат. Kaspersky Security Center не может подключиться к серверу SIEM-системы, если доменное имя сервера SIEM-системы не совпадает с именем субъекта сертификата сервера SIEM-системы. Однако сервер SIEM-системы может изменить свое доменное имя, если имя изменилось в сертификате. В этом случае вы можете указать имена субъектов в поле **Добавить имя субъекта/альтернативное имя субъекта**. Если какое-либо из указанных имен субъектов совпадает с именем субъекта сертификата SIEM-системы, Kaspersky Security Center проверяет сертификат сервера SIEM-системы.

- **Добавить проверку подлинности клиента**

  Для аутентификации клиента вы можете вставить свой сертификат или сгенерировать его в Kaspersky Security Center.

  - **Вставить сертификат**. Вы можете использовать сертификат, полученный из любого источника, например, от любого доверенного центра сертификации. Вам нужно указать сертификат и его закрытый ключ, используя один из следующих типов сертификатов:

    - **X.509-сертификат PEM**. Загрузите файл с сертификатом в поле **Файл с сертификатом** и файл с закрытым ключом в поле **Файл с ключом**. Оба файла не зависят друг от друга. Порядок загрузки файлов не имеет значения. Когда оба файла будут загружены, укажите пароль для расшифровки закрытого ключа в поле **Проверка пароля или сертификата**. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

    - **X.509-сертификат PKCS12**. Загрузите один файл, содержащий сертификат и его закрытый ключ, в поле **Файл с сертификатом**. Когда файл будет загружен, укажите пароль для расшифровки закрытого ключа в поле **Проверка пароля или сертификата**. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

  - **Сгенерировать ключ**. Вы можете сгенерировать самоподписанный сертификат в Kaspersky Security Center. В результате Kaspersky Security Center сохраняет сгенерированный самоподписанный сертификат, и вы можете передать публичную часть сертификата или SHA1-отпечаток в SIEM-систему.

- **Формат данных**

  Вы можете выбрать форматы Kaspersky SIEM (KUMA), IBM QRadar SIEM, ArcSight, Splunk или Syslog в зависимости от требований SIEM-системы.

Если вы выбрали формат данных Syslog, необходимо указать:

- **Максимальный размер сообщения в байтах**

  Укажите максимальный размер в байтах одного сообщения, передаваемого в SIEM-систему. Каждое событие передается одним сообщением. Если реальная длина сообщения превышает указанное значение, сообщение обрезается и данные могут быть утеряны. По умолчанию размер сообщения составляет 2048 байт. Это поле доступно, только если вы выбрали формат Syslog в поле **Протокол**.

5. Заархивированные события можно экспортировать из базы данных Сервера администрирования и задать начальную дату, с которой вы хотите начать экспорт заархивированных событий:

   a. Перейдите по ссылке **Установите дату начала экспорта**.

   b. В открывшемся разделе укажите дату начала в поле **Дата начала экспорта системных событий**.

   c. Нажмите на кнопку **ОК**.

6. Переключите параметр в положение **Автоматически экспортировать события в базу SIEM-системы Включено**.

7. Чтобы убедиться, что соединение с SIEM-системой настроено, нажмите на кнопку **Проверить подключение**.

   Соединение с сервером SIEM-системы установлено, и отправлено тестовое событие. Отобразится статус подключения.

   > Проверка выполняется только для протоколов TCP и TLS over TCP.

8. Нажмите на кнопку **Сохранить**.

Экспорт в SIEM-систему настроен.

Экспорт событий напрямую из базы данных

Вы можете извлекать события напрямую из базы данных Kaspersky Security Center, не используя интерфейс Kaspersky Security Center. Можно создавать запросы непосредственно к публичным представлениям и извлекать из них данные о событиях или создавать собственные представления на базе существующих публичных представлений и обращаться к ним для получения требуемых данных.

Публичные представления

Для вашего удобства в базе данных Kaspersky Security Center предусмотрен набор публичных представлений. Описание публичных представлений приведено в документе klakdb.chm.

Публичное представление v_akpub_ev_event содержит набор полей, соответствующих параметрам событий в базе данных. В документе klakdb.chm также содержится информация о публичных представлениях, относящихся к другим объектам Kaspersky Security Center, например, устройствам, приложениям, пользователям. Вы можете использовать эту информацию при создании запросов.

В этом разделе приведены инструкции по выполнению SQL-запроса с помощью утилиты klsql2, а также пример такого запроса.

Вы также можете использовать любые другие приложения для работы с базами данных для создания SQL-запросов и представлений баз данных. Информация о том, как посмотреть параметры подключения к базе данных Kaspersky Security Center, например, имя инстанса и имя базы данных, приведена в соответствующем разделе.

Выполнение SQL-запроса с помощью утилиты klsql2

В этой статье приведены инструкции по использованию утилиты klsql2, а также по выполнению SQL-запроса с использованием этой утилиты.

Чтобы использовать утилиту klsql2:

1. Найдите утилиту klsql2 в папке установки Kaspersky Security Center. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. Не используйте версии утилиты klsql2, предназначенные для старых версий Kaspersky Security Center.

2. Создайте файл с расширением .sql в любом текстовом редакторе и поместите файл в одну папку с утилитой.

3. В созданном файле .sql введите требуемый SQL-запрос и сохраните файл.

4. На устройстве, на котором установлен Сервер администрирования Kaspersky Security Center, в командной строке введите следующую команду для выполнения SQL-запроса из файла .sql и сохранения результатов в файл result.xml:

   ```
   klsql2 -i src.sql -u <имя пользователя> -p <пароль> -o result.xml
   ```

   где `<имя пользователя>` и `<пароль>` являются учетными данными учетной записи пользователя, имеющего доступ к базе данных.

5. При необходимости введите имя учетной записи и пароль пользователя, имеющего доступ к базе данных.

6. Откройте созданные файлы result.xml и просмотрите результаты выполнения SQL-запроса.

Вы можете изменять файл .sql и создавать в нем любые SQL-запросы к публичным представлениям. Затем с помощью команды в командной строке можно запустить SQL-запрос и сохранить результаты в файл.

Пример SQL-запроса, созданного с помощью утилиты klsql2

В этом разделе приведен пример SQL-запроса, выполненного с помощью утилиты klsql2.

Следующие примеры показывают, как получить список событий, зарегистрированных на устройствах пользователей за последние семь дней, и отсортировать их по времени возникновения. Сначала отображаются самые последние события.

Пример для Microsoft SQL Server:

```
SELECT
  /* идентификатор события */
  e.nId,

  /* время возникновения события */
  e.tmRiseTime,

  /* внутреннее имя типа события  */
  e.strEventType,

  /* отображаемое имя события */
  e.wstrEventTypeDisplayName,

  /* отображаемое описание события */
  e.wstrDescription,

  /* имя группы, в которую входит устройство */
  e.wstrGroupName,

  /* отображаемое имя устройства, на котором произошло событие  */
  h.wstrDisplayName,
  CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

    /* IP-адрес устройства, на котором произошло событие */
  CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
  INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Пример для PostgreSQL:

```
SELECT
  /* идентификатор события */
  "e"."nId",

  /* время возникновения события */
  "e"."tmRiseTime",

  /* внутреннее имя типа события */
  "e"."strEventType",

  /* отображаемое имя события */
  "e"."wstrEventTypeDisplayName",

  /* отображаемое описание события */
  "e"."wstrDescription",

  /* отображаемое описание события */
  "e"."wstrGroupName",

  /* отображаемое имя устройства, на котором произошло событие */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* IP-адрес устройства, на котором произошло событие */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

Пример для MySQL или MariaDB:

```
SELECT

  /* идентификатор события */
  `e`.`nId`,

  /* время возникновения события */
  `e`.`tmRiseTime`,
```

```
    /* внутреннее имя типа события  */
    `e`.`strEventType`,

    /* отображаемое имя события */
    `e`.`wstrEventTypeDisplayName`,

    /* отображаемое описание события */
    `e`.`wstrDescription`,

    /* имя группы устройств */
    `e`.`wstrGroupName`,

    /* отображаемое имя устройства, на котором произошло событие  */
    `h`.`wstrDisplayName`,
    CONCAT(
      LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
      LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
      LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

      /* IP-адрес устройства, на котором произошло событие */
      LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
    )  AS `strIp`
  FROM `v_akpub_ev_event`  AS `e`
    INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
  WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
  ORDER BY `e`.`tmRiseTime` DESC ;
```

Просмотр имени базы данных Kaspersky Security Center

Для доступа к базе данных Kaspersky Security Center с помощью SQL Server, MySQL, или MariaDB необходимо знать имя базы данных, чтобы иметь возможность подключиться к ней из редактора скриптов SQL.

Чтобы просмотреть имя базы данных Kaspersky Security Center:

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Информация об используемой базе данных**.

Имя базы данных указано в поле **Имя базы данных**. Используйте это имя базы данных для подключения и обращения к базе данных в ваших SQL-запросах.

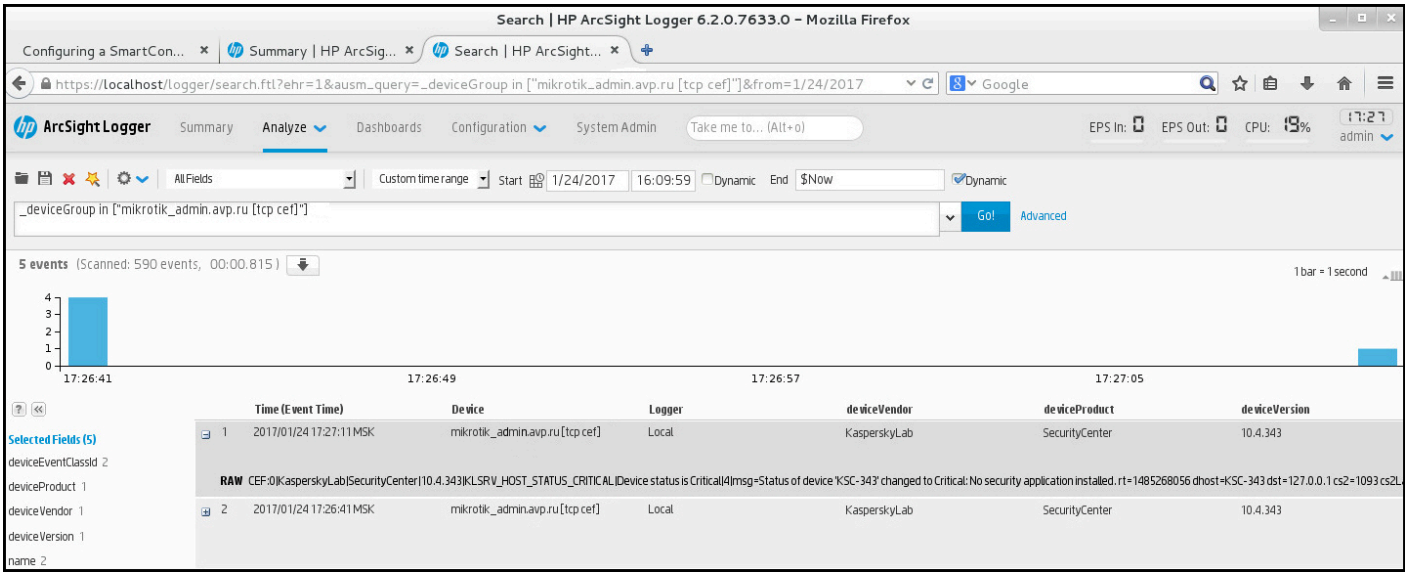
Просмотр результатов экспорта

Вы можете узнать, успешно ли завершилась процедура экспорта. Для этого проверьте, были ли получены SIEM-системой сообщения, содержащие экспортируемые события.

Если отправленные из Kaspersky Security Center события получены и правильно интерпретированы SIEM-системой, значит, настройка на обеих сторонах выполнена корректно. В противном случае проверьте и при необходимости исправьте настройки Kaspersky Security Center и SIEM-системы.

Ниже приведен пример событий, экспортированных в систему ArcSight. Например, первое событие – это критическое событие Сервера администрирования: *Статус устройства "Критический"*.

Отображение экспортированных событий зависит от используемой SIEM-системы.



Пример событий

Работа с Kaspersky Security Center Web Console в облачном окружении

В этом разделе представлена информация о функциях Kaspersky Security Center Web Console, связанных с развертыванием и обслуживанием Kaspersky Security Center 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 отображаются.

Настройка облачного окружения в Kaspersky Security Center Web Console

Чтобы настроить Kaspersky Security Center с использованием мастера настройки облачного окружения, вам потребуется следующее:

- Укажите учетные данные для облачного окружения:
  - IAM-роль, которой было предоставлено право опроса облачного сегмента, или учетная запись IAM-пользователя, которому было 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.

Мастер настройки облачного окружения запускается автоматически при первом подключении к Серверу администрирования через Консоль администрирования, если вы разворачиваете Kaspersky Security Center из готового образа AMI. Вы также можете запустить мастер вручную в любое время.

Чтобы запустить мастер настройки облачного окружения 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 настройки облачного окружения составляет около 15 минут.

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.

- 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.

    Рекомендуется использовать Kaspersky Endpoint Security для Windows вместо Kaspersky Security для Windows Server.

Kaspersky Security Center 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. Лицензирование приложения

Этот шаг отображается только в том случае, если вы используете AMI BYOL и не активировали приложение с помощью лицензии Kaspersky Security для виртуальных сред или лицензии Kaspersky Security для виртуальных и облачных сред.

Укажите лицензионный ключ и нажмите на кнопку **Далее** для продолжения.

Лицензионный ключ добавлен в хранилище Сервера администрирования.

Если вы снова запустите мастер, этот шаг не будет отображаться.

Шаг 3. Выбор облачного окружения и аутентификация

В этом разделе описаны функции, применимые только к приложению версии Kaspersky Security Center 12.1 и выше.

Задайте следующие параметры:

- **Облачное окружение**

  Выберите облачное окружение, в котором вы разворачиваете Kaspersky Security Center: 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, вам потребуется IAM-роль или ключ доступа AWS IAM для дальнейшего опроса облачного сегмента.

- **AWS IAM-роль, назначенная инстансу EC2**

  Выберите этот параметр, если у вас есть IAM-роль с необходимыми правами для Сервера администрирования.

- **AWS IAM-пользователь**

  Выберите этот параметр, если у вас есть ключ доступа AWS IAM. Введите ваши 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, а не IAM-роль.

  - **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, а не IAM-роль.

    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.

- **Ключ доступа хранилища Azure**

  Вы получили пароль (ключ) при создании учетной записи хранения Azure для работы с Kaspersky Security Center.

  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.

- **Приватный 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 облачного окружения позволяет 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 сегмента, настройка синхронизации с облачным окружением и определение дальнейших действий

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 5 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**.

Настройте следующие параметры:

- **Синхронизировать группы администрирования с облачной структурой**

  Если флажок установлен, то внутри группы **Управляемые устройства** автоматически создается группа **AWS** и запускается сканирование облачной сети. Виртуальные машины, обнаруженные во время каждого сканирования облачной сети, перемещаются в группу AWS. Структура подгрупп администрирования внутри группы AWS соответствует структуре вашего облачного сегмента. Устройства, не идентифицированные как инстансы Amazon EC2, находятся в группе **Нераспределенные устройства**. Такая структура групп позволяет устанавливать антивирусные программы на инстансы с помощью задач групповой установки и настраивать разные политики для разных групп.

  Если флажок не установлен, то группа AWS также создается и опрос сети также запускается, однако внутри группы не создаются подгруппы, соответствующие структуре облачного сегмента. Все найденные инстансы находятся в группе администрирования AWS и отображаются единым списком. Если в процессе работы с Kaspersky Security Center вам потребуется произвести синхронизацию, то вы сможете изменить свойства правила **Синхронизация с AWS** и форсировать его. Форсирование правила перестраивает структуру групп внутри группы AWS так, чтобы она соответствовала структуре вашего облачного сегмента.

  По умолчанию флажок снят.

- **Развернуть защиту**

  Если этот флажок установлен, то мастер создает задачу установки защитных программ на инстансы. После завершения работы мастера автоматически запустится мастер развертывания защиты на инстансы EC2 в ваших облачных сегментах, и вы сможете установить на них Агент администрирования и программы защиты.

  Если у IAM-пользователя, от имени которого работает Kaspersky Security Center, или у IAM-роли, которую вы используете, нет прав на установку программ на инстансы, то рекомендуется разворачивать защиту с помощью скриптов развертывания.

  Если флажок снят, то мастер развертывания защиты не запускается и задачи установки защитных программ на инстансы не создаются. Вы можете произвести оба эти действия позже вручную.

  По умолчанию флажок установлен.

Если вы выберете параметр Развернуть защиту, раздел **Перезагрузка устройств** становится доступным. В этом разделе вам нужно выбрать действие, в случае если операционная система целевого устройства должна быть перезагружена. Выберите, перезагружать ли инстансы, если в ходе установки приложений на устройства потребуется перезагрузка операционной системы:

- **Не перезагружать**

  Если выбран этот вариант, устройство не будет перезагружаться после установки приложения безопасности.

- **Перезагрузить**

  Если выбран этот вариант, устройство будет перезагружено после установки приложения безопасности.

Нажмите на кнопку **Далее**, чтобы продолжить.

Вы можете выполнить развертывание Google Cloud только с помощью инструментов Kaspersky Security Center. Если вы выбрали Google Cloud, вариант **Развернуть защиту** недоступен.

Шаг 5. Выбор приложения для создания политики и задач

Этот шаг отображается, только если у вас есть инсталляционные пакеты и плагины как для Kaspersky Endpoint Security для Windows, так и для Kaspersky Security для Windows Server. Если у вас есть плагин и инсталляционный пакет только для одного из этих приложений, этот шаг пропускается и Kaspersky Security Center создает политику и задачи для существующего приложения.

Выберите приложение, для которого требуется создать политику и задачи:

- Kaspersky Endpoint Security для Windows
- Kaspersky Security для Windows Server

Шаг 6. Настройка Kaspersky Security Network для Kaspersky Security Center

Настройте параметры передачи информации о работе Kaspersky Security Center в базу знаний Kaspersky Security Network (KSN). Выберите один из следующих вариантов:

- **Я принимаю условия использования Kaspersky Security Network**

  Kaspersky Security Center и управляемые приложения, установленные на клиентских устройствах, в автоматическом режиме будут предоставлять информацию об их работе Kaspersky Security Network. Сотрудничество с Kaspersky Security Network обеспечивает более быстрое обновление баз данных о вирусах и угрозах, что увеличивает скорость реагирования на возникающие угрозы безопасности.

- **Я не принимаю условия использования Kaspersky Security Network**

  Kaspersky Security Center и управляемые приложения не будут предоставлять информацию о своей работе Kaspersky Security Network.

  Если вы выбрали этот параметр, использование Kaspersky Security Network будет выключено.

"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 7. 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 Web Console

Информацию о структуре сети и входящих в ее состав устройствах Сервер администрирования получает в ходе регулярных опросов облачных сегментов средствами AWS API, Azure API или Google API. На основании полученной информации Kaspersky Security Center 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 Сервер администрирования мог опрашивать облачные сегменты, необходимы соответствующие права, которые обеспечивает IAM-роль или 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 соединений для опроса облачных сегментов

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: 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 следующие параметры:

     - **Использовать AWS IAM-роль**

       Выберите этот вариант, если вы уже создали IAM-роль для работы Сервера администрирования с сервисами AWS.

     - **Учетные данные записи AWS IAM-пользователя**

       Выберите этот вариант, если у вас есть учетная запись IAM-пользователя с необходимыми правами и вы можете ввести ID ключа и секретный ключ.

       Если вы указали, что у вас есть Учетные данные записи AWS IAM-пользователя 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, а не IAM-роль.

       - **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, а не IAM-роль.

       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.

- **Ключ доступа хранилища Azure**

  Вы получили пароль (ключ) при создании учетной записи хранения Azure для работы с Kaspersky Security Center.

  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.

- **Приватный 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 **ОК**, 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 Web Console

Опрос облачного сегмента происходит по расписанию. Вы можете задать периодичность, с которой происходит опрос.

В параметрах мастера настройки облачного окружения автоматически задается периодичность опроса – раз в 5 минут. Вы можете изменить это значение в любое время и задать другое расписание. Не рекомендуется производить опрос чаще, чем раз в 5 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**.

   Откроется 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.

- **Start interval**

  Укажите значение N (для минут или дней).

- **Начиная с**

  Укажите начало первого опроса.

- **Запускать пропущенные задачи**

  Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

  Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

  Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

  По умолчанию параметр включен.

6. Сохраните изменения.

Расписание опроса для сегмента настроено и сохранено.

Просмотр результатов опроса облачного сегмента с помощью Kaspersky Security Center Web 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 Web Console

Вы можете просмотреть свойства каждого облачного устройства.

Чтобы просмотреть свойства облачного устройства:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые 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 настройки облачного окружения 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 использовании функции Настроить облачное окружение 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 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**, а затем примените правило.

4. Выберите значение в раскрывающемся списке **Устройство обнаружено с помощью API**:

   - **Нет**. Устройство не обнаруживается с помощью AWS API, Azure API 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 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
  - Kaspersky Security для Windows Server
- 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.

Чтобы создать задачу удаленной установки приложения на виртуальные машины Azure:

1. В главном окне приложения, перейдите в раздел **Активы (Устройства)** → **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.

Создание задачи резервного копирования данных Сервера администрирования с использованием облачной СУБД

Задачи резервного копирования относятся к задачам Сервера администрирования. Вы создаете задачу резервного копирования данных, если хотите использовать СУБД, расположенную в облачном окружении (AWS или Azure).

Чтобы создать задачу резервного копирования данных Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. На первом шаге мастера в списке **Приложение** выберите **Kaspersky Security Center 15.1** и в списке **Тип задачи** выберите **Резервное копирование данных Сервера администрирования**.
4. На соответствующей странице мастера укажите следующую информацию:

   - Если вы работаете с базой данных в AWS:

     - **Имя корзины S3**

       Имя корзины S3, которое вы создали для резервной копии данных.

     - **ID ключа доступа**

       Вы получили ID ключа (последовательность из букв и цифр), когда создали учетную запись IAM-пользователя для работы с корзиной S3 в хранилище инстансов.

       Поле доступно, если вы выбрали базу RDS для контейнера S3.

     - **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, а не IAM-роль.

   - Если вы работаете с базой данных в Microsoft Azure:

     - **Имя учетной записи хранения Azure**

       Вы создали имя учетной записи хранения Azure для работы с Kaspersky Security Center.

     - **Идентификатор подписки Azure**

       Вы создали подписку на портале Azure.

- **Пароль 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.

- **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.

- **Имя SQL-сервера Azure**

  Имя и группа источника доступны в свойствах SQL-сервера Azure.

- **Группа источника SQL-сервера Azure**

  Имя и группа источника доступны в свойствах SQL-сервера Azure.

- **Ключ доступа хранилища Azure**

  Доступен в свойствах учетной записи хранения в разделе "Access Keys". Вы можете использовать любой ключ (key1 или key2).

Задача будет создана и отобразится в списке задач. Если вы включите параметр **Открыть окно свойств задачи после ее создания**, вы можете изменить параметры задачи по умолчанию сразу после ее создания. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

Удаленная диагностика клиентских устройств

Вы можете использовать удаленную диагностику для удаленного выполнения следующих операций на клиентских устройствах на базе Windows и Linux:

- включения и выключения трассировки, изменения уровня трассировки и загрузки файла трассировки;
- загрузки системной информации и параметров приложения;
- загрузки журналов событий;
- создание файла дампа для приложения;
- запуска диагностики и загрузки результатов диагностики;
- запуск, остановка и перезапуск приложений.

Вы можете использовать журнал событий и диагностические отчеты, загруженные с клиентского устройства, для устранения неполадок самостоятельно. Также если вы обращаетесь в Службу технической поддержки "Лаборатории Касперского", специалист технической поддержки "Лаборатории Касперского" может попросить вас загрузить файлы трассировки, файлы дампа, журнал событий и диагностические отчеты с клиентского устройства для дальнейшего анализа в "Лаборатории Касперского".

Открытие окна удаленной диагностики

Чтобы выполнить удаленную диагностику клиентских устройств на базе Windows и на базе Linux, сначала нужно открыть окно удаленной диагностики.

Чтобы открыть окно удаленной диагностики:

1. Чтобы выбрать устройство, для которого вы хотите открыть окно удаленной диагностики, выполните одно из следующих действий:

   - Если устройство принадлежит к группе администрирования, в главном меню перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.

   - Если устройство принадлежит к группе нераспределенных устройств, в главном меню перейдите в раздел **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.

2. Нажмите на имя требуемого устройства.

3. В открывшемся окне свойств устройства выберите вкладку **Дополнительно**.

4. В появившемся окне нажмите на кнопку **Удаленная диагностика**.

   В результате открывается окно **Удаленная диагностика** клиентского устройства. Если отсутствует соединение между Сервером администрирования и клиентским устройством, появится сообщение об ошибке.

Если вам нужно получить сразу всю диагностическую информацию о клиентском устройстве с операционной системой Linux, вы можете запустить на этом устройстве скрипт collect.sh.

Включение и выключение трассировки для приложений

Вы можете включать и выключать трассировку для приложений, включая трассировку xperf.

Включение и выключение трассировки

Чтобы включить или выключить трассировку на удаленном устройстве:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.

3. В списке приложений выберите приложение, для которого требуется включить или выключить трассировку.

   Откроется список параметров удаленной диагностики.

4. Если вы хотите включить трассировку:

   a. В разделе **Трассировка** нажмите на кнопку **Включить трассировку**.

   b. В открывшемся окне **Изменить уровень трассировки** рекомендуется не менять значения, заданные по умолчанию. При необходимости специалист Службы технической поддержки проведет вас через процесс настройки. Доступны следующие параметры:

   - **Уровень трассировки**

     Уровень трассировки определяет состав информации, которую содержит файл трассировки.

   - **Трассировка на основе ротации**

     Приложение перезаписывает информацию трассировки, чтобы предотвратить чрезмерное увеличение файла трассировки. Укажите максимальное количество файлов, которые будут использоваться для хранения информации трассировки, и максимальный размер каждого файла. Если записано максимальное количество файлов трассировки максимального размера, самый старый файл трассировки будет удален, чтобы можно было записать новый файл трассировки.

     Этот параметр доступен только для Kaspersky Endpoint Security.

   c. Нажмите на кнопку **Сохранить**.

   Трассировка включена для выбранного приложения. В некоторых случаях для включения трассировки приложения безопасности требуется перезапустить это приложение и его задачу.

   > На клиентских устройствах под управлением Linux трассировка компонента Обновление Агента администрирования регулируется параметрами Агента администрирования. Поэтому параметры **Включить трассировку** и **Изменить уровень трассировки** выключены для этого компонента на клиентских устройствах под управлением Linux.

5. Если вы хотите выключить трассировку для выбранного приложения, нажмите на кнопку **Выключить трассировку**.

   Трассировка выключена для выбранного приложения.

Включение трассировки Xperf

Для Kaspersky Endpoint Security специалисты Службы технической поддержки могут попросить вас включить трассировку Xperf для получения информации о производительности системы.

Чтобы включить, настроить или отключить трассировку Xperf:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.

3. В списке приложений выберите Kaspersky Endpoint Security для Windows.

   Откроется список параметров удаленной диагностики для Kaspersky Endpoint Security для Windows.

4. В разделе **Трассировка Xperf** нажмите на кнопку **Включить трассировку Xperf**.

   Если трассировка Xperf уже включена, отображается кнопка **Выключить трассировку Xperf**. Нажмите на эту кнопку, если хотите отключить трассировку Xperf для Kaspersky Endpoint Security для Windows.

5. В открывшемся окне **Изменить уровень трассировки Xperf**, в зависимости от запроса специалиста Службы технической поддержки, выполните следующее:

   a. Выберите один из уровней трассировки:

   - **Легкий уровень**

     Файл трассировки этого типа содержит минимальный объем информации о системе.

     По умолчанию выбран этот вариант.

   - **Детальный уровень**

     Файл трассировки этого типа содержит более подробную информацию, чем файл типа *Легкий уровень*, и может запрашиваться специалистами Технической поддержки, если информации в файле трассировки *легкого уровня* недостаточно для оценки производительности. Файл трассировки *Детального уровня* содержит информацию об оборудовании, операционной системе, список запущенных и завершенных процессов и приложений, событиях, используемых для оценки производительности, а также события Средства оценки системы Windows.

   b. Выберите один из уровней трассировки Xperf:

   - **Базовый тип**

     Приложение получает данные трассировки во время работы приложения Kaspersky Endpoint Security.

     По умолчанию выбран этот вариант.

   - **Тип перезагрузки**

     Приложение получает данные трассировки, когда на управляемом устройстве запускается операционная система. Этот тип трассировки эффективен, когда проблема, влияющая на производительность системы, возникает после включения устройства и перед запуском Kaspersky Endpoint Security.

   Также вам могут предложить включить параметр **Размер файлов ротации (МБ)**, чтобы предотвратить чрезмерное увеличение файла трассировки. Затем укажите максимальный размер файла трассировки. Когда файл достигает максимального размера, самый старый файл трассировки будет перезаписан новым файлом.

   c. Определите размер файла ротации.

   d. Нажмите на кнопку **Сохранить**.

   Трассировка Xperf включена и настроена.

6. Если вы хотите отключить трассировку Xperf для Kaspersky Endpoint Security для Windows, нажмите **Выключить трассировку Xperf** в разделе **Трассировка Xperf**.

   Трассировка Xperf выключена.

Загрузка файла трассировки приложения

Чтобы загрузить файл трассировки приложения:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В списке приложений выберите приложение, для которого вы хотите загрузить файл трассировки.
4. В разделе **Трассировка** нажмите на кнопку **Файлы трассировки**.

   Откроется окно **Журналы удаленной установки**, где отображается список файлов трассировки.
5. В списке файлов трассировки выберите файл, который вы хотите загрузить.
6. Выполните одно из следующих действий:

   - Загрузите выбранный файл, нажав на кнопку **Загрузить**. Вы можете выбрать один или несколько файлов для загрузки.
   - Загрузите часть выбранного файла:

     a. Нажмите на кнопку **Загрузить часть**.

     Одновременная частичная загрузка нескольких файлов невозможна. Если вы выберете более одного файла трассировки, кнопка **Загрузить часть** будет неактивна.

     b. В открывшемся окне укажите имя и часть файла для загрузки в соответствии с вашими требованиями.

     Для устройств под управлением Linux изменение имени части файла недоступно.

     c. Нажмите на кнопку **Загрузить**.

Выбранный файл или его часть загружается в указанное вами расположение.

Удаление файлов трассировки

Вы можете удалить файлы трассировки, которые больше не нужны.

Чтобы удалить файл трассировки, выполните следующее действие:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В открывшемся окне удаленной диагностики выберите раздел **Журналы событий**.
3. В разделе **Файлы трассировки** нажмите **Журналы службы Центра обновления Windows** или **Журналы удаленной установки**, в зависимости от того, какие файлы трассировки вы хотите удалить.

Ссылка **Журналы службы Центра обновления Windows** доступна только для клиентских устройств под управлением Windows.

Откроется окно **Журналы событий трассировки устройства**, где отображается список файлов трассировки.

4. В списке файлов трассировки выберите один или несколько файлов, которые вы хотите удалить.
5. Нажмите на кнопку **Удалить**.

Выбранные файлы трассировки удалены.

Загрузка параметров приложений

Чтобы загрузить с клиентского устройства параметры приложений:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.
3. В разделе **Параметры приложения** нажмите на кнопку **Загрузить** для загрузки информации о параметрах приложений, установленных на клиентском устройстве.

ZIP-архив с информацией загрузится в указанное расположение.

Загрузка журналов событий

Чтобы загрузить с удаленного устройства журнал событий:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В разделе **Журналы событий** в окне удаленной диагностики выберите **Журнал событий всех устройств**.
3. В окне **Журнал событий всех устройств** выберите один или несколько журналов событий.
4. Выполните одно из следующих действий:
   - Загрузите выбранный журнал событий, нажав на кнопку **Загрузить весь файл**.
   - Загрузите часть выбранного журнала событий:
     a. Нажмите на кнопку **Загрузить часть**.

     Одновременная частичная загрузка нескольких журналов событий невозможна. Если вы выберете более одного журнала событий, кнопка **Загрузить часть** будет неактивна.

b. В открывшемся окне укажите имя и часть журнала событий для загрузки в соответствии с вашими требованиями.

Для устройств под управлением Linux изменение имени части журнала событий недоступно.

c. Нажмите на кнопку **Загрузить**.

Выбранный журнал событий или его часть загрузится в указанное расположение.

Запуск, остановка и перезапуск приложения

Вы можете запускать, останавливать и перезапускать приложения на клиентском устройстве.

Чтобы запустить, остановить или перезапустить приложение:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В списке приложений выберите приложение, которое вы хотите запустить, остановить или перезапустить.
4. Выберите действие, нажав на одну из следующих кнопок:

   - **Остановить приложение**

     Эта кнопка доступна, только если приложение в данный момент запущено.
   - **Перезапустить приложение**

     Эта кнопка доступна, только если приложение в данный момент запущено.
   - **Запустить приложение**

     Эта кнопка доступна, только если приложение в данный момент не запущено.

   В зависимости от выбранного вами действия требуемое приложение запустится, остановится или перезапустится на клиентском устройстве.

Если вы перезапустите Агент администрирования, появится сообщение о том, что текущее соединение устройства с Сервером администрирования будет потеряно.

Запуск удаленной диагностики Агента администрирования Kaspersky Security Center и скачивание результатов

Чтобы запустить диагностику Агента администрирования Kaspersky Security Center на удаленном устройстве и загрузить ее результаты:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В разделе списке приложений выберите **Агент администрирования Kaspersky Security Center**.

   Откроется список параметров удаленной диагностики.
4. В разделе **Отчет диагностики** нажмите на кнопку **Выполнить диагностику**.

   Запускается процесс удаленной диагностики и генерируется отчет о диагностике. По завершении процесса диагностики кнопка **Загрузить отчет диагностики** становится доступной.
5. Нажмите на кнопку **Загрузить отчет диагностики**, чтобы загрузить отчет.

Отчет загрузится в указанное расположение.

Запуск приложения на клиентском устройстве

Вам может потребоваться запустить приложение на клиентском устройстве, если вас об этом попросит специалист Службы технической поддержки "Лаборатории Касперского". Вам не нужно устанавливать приложение самостоятельно на этом устройстве.

Чтобы запустить приложение на клиентском устройстве:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Запуск удаленного приложения**.
3. В разделе **Файлы приложения** нажмите на кнопку **Обзор** для выбора ZIP-архива с приложением, которое вы хотите запустить на клиентском устройстве.

   > ZIP-архив должен содержать папку утилиты. Эта папка содержит исполняемый файл для запуска на удаленном устройстве.

   При необходимости можно указать имя исполняемого файла и аргументы командной строки. Для этого заполните поля **Исполняемый файл в архиве для запуска на удаленном устройстве** и **Аргументы командной строки**.
4. Нажмите на кнопку **Загрузить и запустить** для запуска указанного приложения на клиентском устройстве.
5. Следуйте указаниям сотрудника службы поддержки "Лаборатории Касперского".

Создание файла дампа для приложения

Файл дампа приложения позволяет просматривать параметры приложения, работающего на клиентском устройстве, в определенный момент времени. Этот файл также содержит информацию о модулях, которые были загружены для приложения.

Получение файлов дампа с клиентских устройств с операционной системой Linux не поддерживается.

Чтобы получить файлы дампа с помощью удаленной диагностики, используется утилита kldumper. Эта утилита предназначена для получения файлов дампа процессов приложений "Лаборатории Касперского" по запросу экспертов Службы технической поддержки. Подробная информация о требованиях к использованию утилиты kldumper приведена в Базе знаний Kaspersky Security Center.

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 дампа процесса** укажите исполняемый файл приложения, для которого вы хотите создать файл дампа.
4. Нажмите на кнопку **Загрузить дамп файла**.

   Архив с файлом дампа для указанного приложения загружен.

   Если указанное приложение не запущено на клиентском устройстве, папка "result" в загруженном архиве будет пустой.

   Если указанное приложение запущено, но загрузка завершается с ошибкой или папка "result" в загруженном архиве пуста, см. Базу знаний Kaspersky Security Center.

Запуск удаленной диагностики на клиентском устройстве с операционной системой Linux

Kaspersky Security Center позволяет загружать основную диагностическую информацию с клиентского устройства. Кроме того, вы можете получить диагностическую информацию об устройстве с операционной системой Linux с помощью скрипта collect.sh "Лаборатории Касперского". Этот скрипт запускается на клиентском устройстве с операционной системой Linux, которое необходимо диагностировать. Затем создается файл с диагностической информацией, системной информацией об этом устройстве, файлами трассировки приложений, журналами событий устройства и файлом дампа для аварийных ситуаций, прерванных приложений.

Рекомендуется использовать скрипт collect.sh для получения сразу всей диагностической информации о клиентском устройстве с операционной системой Linux. Если вы загружаете диагностическую информацию удаленно через Kaspersky Security Center, вам нужно будет пройти все разделы интерфейса удаленной диагностики. Кроме того, диагностическая информация для устройства с операционной системой Linux, вероятно, не будет получена полностью.

Если вам необходимо отправить сформированный файл с диагностической информацией в Службу технической поддержки "Лаборатории Касперского", удалите всю конфиденциальную информацию перед отправкой файла.

Чтобы загрузить диагностическую информацию с клиентского устройства с операционной системой Linux с помощью скрипта collect.sh:

1. Загрузите скрипт collect.sh, который запакован в архив collect.tar.gz.
2. Скопируйте загруженный архив на клиентское устройство с операционной системой Linux, которое необходимо диагностировать.
3. Выполните следующую команду, чтобы распаковать архив collect.tar.gz:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Выполните следующую команду, чтобы указать права на выполнение скрипта:

   ```
   # chmod +x collect.sh
   ```

5. Запустите сценарий collect.sh под учетной записью с правами администратора:

   ```
   # ./collect.sh
   ```

Файл с диагностической информацией будет сформирован и сохранен в папке /tmp/$HOST_NAME-collect.tar.gz.

Загрузка и удаление файлов из разделов Карантин и Резервное хранилище

В этом разделе представлена информация о том, как загрузить и удалить файлы из разделов Карантин и Резервное хранилище в Kaspersky Security Center Web Console.

Загрузка файлов из разделов Карантин и Резервное хранилище

Вы можете загрузить файлы из Карантина и Резервного хранилища, только если выполняется одно из двух условий: либо включен параметр **Не разрывать соединение с Сервером администрирования** в свойствах устройства, либо используется шлюз соединения. Иначе загрузка невозможна.

Чтобы сохранить копию файла из раздела Карантин или Резервное хранилище на жесткий диск:

1. Выполните одно из следующих действий:

   - Если вы хотите сохранить копию файла из Карантина, в главном меню перейдите в раздел **Операции** → **Хранилища** → **Карантин**.

   - Если вы хотите сохранить копию файла из Резервного хранилища, в главном меню перейдите в раздел **Операции** → **Хранилища** → **Резервное хранилище**.

2. В открывшемся окне выберите файл, который вы хотите загрузить, и нажмите **Загрузить**.

   Начнется загрузка. Копия файла, помещенного в Карантин на клиентском устройстве, сохраняется в указанную папку.

Изменение языка интерфейса Kaspersky Security Center Web Console

Вы можете выбрать один из поддерживаемых языков локализации в качестве языка интерфейса Kaspersky Security Center Web Console.

Чтобы изменить язык интерфейса:

1. В главном окне приложения перейдите в раздел **Параметры** → **Язык**.

2. Выберите необходимый язык интерфейса.

Справочное руководство API

Справочное руководство по Kaspersky Security Center OpenAPI предназначено для решения следующих задач:

- Автоматизация и настройка. Вы можете автоматизировать задачи, которые, возможно, не хотите выполнять вручную, с помощью Консоли администрирования. Вы также можете использовать собственные сценарии, которые еще не поддерживаются в Консоли администрирования. Например, как администратор вы можете использовать Kaspersky Security Center OpenAPI для создания и запуска сценариев, которые упростят разработку структуры групп администрирования и поддержат ее в актуальном состоянии.

- Пользовательская разработка. Например, вы можете разработать альтернативную Консоль администрирования на основе консоли Microsoft Management Console (MMC) для своих клиентов, которая разрешает ограниченный набор действий.

Вы можете использовать поле поиска в правой части экрана, чтобы найти нужную информацию в справочном руководстве OpenAPI.

Справочное руководство OpenAPI

Примеры сценариев

Справочное руководство по OpenAPI содержит примеры сценариев Python, перечисленные в таблице ниже. Примеры показывают, как вы можете вызывать методы OpenAPI и автоматически выполнять различные задачи по защите вашей сети, например, создавать иерархию "главный/подчиненный", запускать задачи в Kaspersky Security Center или назначать точки распространения. Вы можете запускать примеры как есть или создавать собственные сценарии на их основе.

Чтобы вызвать методы OpenAPI и запустить сценарии:

1. Скачайте архив KlAkOAPI.tar.gz. Этот архив включает в себя пакет KlAkOAPI и примеры (их можно скопировать из архива или справочного руководства по OpenAPI). Также архив KlAkOAPI.tar.gz находится в папке установки Kaspersky Security Center.

2. Установите пакет KlAkOAPI из архива KlAkOAPI.tar.gz на устройстве, на котором установлен Сервер администрирования.

   Вызывать методы OpenAPI, запускать примеры и свои сценарии можно только на устройствах, на которых установлены Сервер администрирования и пакет KlAkOAPI.

Пример	Назначение примера	Сценарий
Журнал событий KlAkParams	Вы можете извлекать и обрабатывать данные, используя `KlAkParams` структуру данных. В примере показано, как работать с этой структурой данных. Пример вывода может быть представлен по-разному. Вы можете получить данные для отправки HTTP-метода или использовать их в своем коде.	Мониторинг и отчеты
Создание и удаление иерархии "главный/подчиненный"	Вы можете добавить подчиненный Сервер администрирования и установить таким образом отношение иерархии "главный Сервер – подчиненный Сервер". Или вы можете исключить подчиненный Сервер администрирования из иерархии.	• Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования • Удаление иерархии Серверов администрирования
Создайте иерархию группы со структурой на основе подразделения Active Directory.	Вы можете выполнить опрос подразделения Active Directory и сформировать иерархию обнаруженных групп устройств.	Создание групп администрирования
Создайте иерархию группы со структурой на основе кешированного подразделения Active Directory.	Вы можете сформировать иерархию групп управляемых устройств на основе ранее выполненного опроса подразделения Active Directory. Если новые устройства появляются в Active Directory после последнего опроса, они будут добавлены в группу, так как их нет в сохраненных результатах опроса.	Создание групп администрирования
Загрузите файлы списка сетей с помощью шлюза соединения на указанное устройство	Вы можете подключиться к Агенту администрирования на нужном устройстве, используя шлюз соединения, а затем загрузить файл со списком сетей на свой компьютер.	Настройка точек распространения и шлюзов соединений
Установить лицензионный ключ, хранящийся в хранилище главного Сервера администрирования, на подчиненные Серверы администрирования	Вы можете подключиться к главному Серверу администрирования, загрузить с него необходимый лицензионный ключ и передать этот ключ на все подчиненные Серверы администрирования, входящие в иерархию.	Лицензирование управляемых приложений
Создайте отчет об эффективных правах пользователей	Вы можете создать разные отчеты. Например, вы можете сгенерировать отчет об эффективных правах пользователя, используя этот пример. В этом отчете представлена информация о правах, которыми обладает пользователь в зависимости от его группы и роли. Вы можете загрузить отчет в формате HTML, PDF или Excel.	Генерация и просмотр отчета
Запуск задачи на устройстве	Вы можете подключиться к Агенту администрирования на нужном устройстве, используя шлюз соединения, а затем запустить необходимую задачу.	Запуск задачи вручную
Создание IP-подсетей на основе сайта и служб Active Directory	Вы можете создать IP-подсеть на основе используемого подразделения Active Directory. В примере запускается опрос указанного диапазона IP-адресов и удаляются обнаруженные подсети, чтобы избежать их конфликта с новой подсетью. Поэтому не запускайте такой пример в сети, где важно сохранить подсети. После опроса пример кода обращается к Active Directory, проверяет каждое устройство в нем и создает IP-подсеть. Для этого в примере используются маски и IP-адреса всех устройств.	Настройка защиты сети
Регистрация точек распространения для устройств в группе	Вы можете назначить управляемые устройства точками распространения (ранее они назывались "агенты обновлений").	Обновление баз и приложений "Лаборатории Касперского"

Пример	Назначение примера	Сценарий
Перечисление всех групп	Вы можете выполнять различные действия с группами администрирования. В примере показано, как выполнить следующее: • Получить идентификатор корневой группы "Управляемые устройства". • Переместить по иерархии групп. • Получить полную развернутую иерархию групп с их именами и вложенностью.	Настройка Сервера администрирования
Перечисление задач, запрос статистики задач и запуск задач	Вы можете ознакомиться со следующей информацией: • Историей выполнения задачи. • Текущим статусом задачи. • Количеством задач в разных статусах. Вы также можете запустить задачу. По умолчанию пример запускает задачу после вывода статистики.	Наблюдение за ходом выполнения задачи
Создание и запуск задачи	Вы можете создать задачу. Укажите в примере следующие параметры задачи: • Тип. • Способ запуска. • Имя. • Группа устройств, для которой будет использоваться задача. По умолчанию в примере создается задача типа "Показать сообщение". Вы можете запустить эту задачу для всех управляемых устройств Сервера администрирования. При необходимости вы можете указать свои параметры задачи.	Создание задачи
Перечисление лицензионных ключей	Вы можете получить список всех активных лицензионных ключей для приложений "Лаборатории Касперского", установленных на управляемых устройствах Сервера администрирования. Список содержит подробные сведения о каждом лицензионном ключе, такие как имя, тип или срок действия.	Просмотр информации об используемых лицензионных ключах
Создание и поиск внутреннего пользователя	Вы можете создать учетную запись для дальнейшей работы.	Выбор учетной записи для запуска Сервера администрирования
Создание пользовательской категории	Вы можете создать категорию приложений с требуемыми параметрами.	Создание пополняемой вручную категории приложений
Перечисление пользователей с помощью SrvView	Вы можете использовать класс SrvView для запроса подробной информации с Сервера администрирования. Например, вы можете получить список пользователей, используя этот пример.	Управление учетными записями пользователей

Приложения, взаимодействующие с Kaspersky Security Center через OpenAPI

Некоторые приложения взаимодействуют с Kaspersky Security Center через OpenAPI. К таким приложениям относятся, например, Kaspersky Anti Targeted Attack Platform или Kaspersky Security для виртуальных сред. Это также может быть пользовательское клиентское приложение, разработанное вами на основе OpenAPI.

Приложения, взаимодействующие с Kaspersky Security Center через OpenAPI, подключаются к Серверу администрирования. Если вы настроили список разрешенных IP-адресов для подключения к Серверу администрирования, добавьте IP-адреса устройств, на которых установлены приложения, использующие Kaspersky Security Center OpenAPI. Чтобы узнать, работает ли используемое вами приложение с OpenAPI, обратитесь к справке этого приложения.

Лучшие практики для поставщиков услуг

В этой справке вы найдете информацию о настройке и использовании Kaspersky Security Center.

Документ содержит рекомендации по развертыванию, настройке и использованию приложения, а также способы решения типичных проблем, возникающих при работе приложения.

Планирование развертывания Kaspersky Security Center

Планируя развертывание компонентов Kaspersky Security Center в сети организации, следует принимать во внимание размер и масштаб проекта, а также следующие факторы:

- общего количества устройств;
- количество MSP-клиентов.

Один Сервер администрирования может обслуживать не более чем 100 000 устройств. Если общее количество устройств в сети организации превышает 100 000, следует разместить на стороне MSP несколько Серверов администрирования, объединенных в иерархию для удобства централизованного управления.

На одном Сервере администрирования может быть создано до 500 виртуальных Серверов, следовательно, на каждые 500 MSP-клиентов необходим отдельный Сервер администрирования.

На этапе планирования развертывания следует рассмотреть необходимость задания Серверу администрирования специального сертификата X.509. Задание сертификата X.509 для Сервера администрирования может быть целесообразно в следующих случаях (неполный список):

- для инспекции SSL трафика посредством SSL termination proxy;
- для задания желательных значений полей сертификата;
- для обеспечения желаемой криптографической стойкости сертификата.

Предоставление доступа к Серверу администрирования из интернета

Для того чтобы устройства, размещенные в сети клиента, могли обращаться к Серверу администрирования через интернет, необходимо сделать доступными следующие порты Сервера администрирования:

- 13000 TCP – порт TLS Сервера администрирования, к данному порту подключаются Агенты администрирования, размещенные в сети клиента;
- 8061 TCP – порт HTTPS, используется для публикации автономных пакетов средствами Консоли администрирования;

- 8060 TCP – порт HTTPS, используется для публикации автономных пакетов средствами Консоли администрирования;

- 13292 TCP – данный TLS-порт нужен, только если требуется управлять мобильными устройствами.

В случае если необходимо предоставить клиентам базовые возможности по администрированию своей сети посредством Kaspersky Security Center Web Console, то также необходимо открыть порт 8080 TCP (HTTPS-порт) Kaspersky Security Center Web Console.

Типовая конфигурация Kaspersky Security Center

На серверах MSP размещен один или несколько Серверов администрирования. Количество Серверов может быть выбрано как исходя из наличия доступного аппаратного обеспечения, так и в зависимости от количества обслуживаемых MSP-клиентов или же общего количества управляемых устройств.

Один Сервер администрирования может обслуживать до 100 000 устройств. Вам нужно учесть возможность увеличения количества управляемых устройств в ближайшем будущем: может оказаться желательным подключение несколько меньшего количества устройств к одному Серверу администрирования.

На одном Сервере администрирования может быть создано до 500 виртуальных Серверов, следовательно, на каждые 500 MSP-клиентов необходим отдельный Сервер администрирования.

Если Серверов несколько, рекомендуется объединить их в иерархию. Наличие иерархии Серверов администрирования позволяет избежать дублирования политик и задач, работать со всем множеством управляемых устройств, как если бы они все управлялись одним Сервером администрирования: выполнять поиск устройств, создавать выборки устройств, создавать отчеты.

На каждом виртуальном Сервере, соответствующем MSP-клиенту, следует назначить по одной или по несколько точек распространения. Так как связь между MSP-клиентами и Сервером администрирования осуществляется через интернет, целесообразно создать для точек распространения задачу *Загрузка обновлений в хранилища точек распространения* так, чтобы точки распространения загружали обновления не с Сервера администрирования, а непосредственно с серверов "Лаборатории Касперского".

Если в сети MSP-клиента часть устройств не имеет прямого доступа в интернет, то точки распространения следует переключить в режим шлюза соединения. В таком случае Агенты администрирования на устройствах в сети MSP-клиента будут подключаться (с целью синхронизации) к Серверу администрирования не напрямую, а через шлюз.

Поскольку Сервер администрирования не может выполнять опрос сети MSP-клиента, целесообразно возложить выполнение этой функции на одну из точек распространения.

Сервер администрирования не сможет посылать уведомления на порт 15000 UDP управляемым устройствам, размещенным за NAT в сети MSP-клиента. Для решения этой проблемы целесообразно включить в свойствах устройств, являющихся точками распространения и работающих в режиме шлюза соединений, режим постоянного соединения с Сервером администрирования (флажок **Не разрывать соединение с Сервером администрирования**). Режим постоянного соединения доступен, если общее количество точек распространения не превышает 300.

О точках распространения

Устройства с установленным Агентом администрирования могут быть использованы в качестве точки распространения. В этом режиме Агент администрирования может выполнять следующие функции:

- Передачу файлов на клиентские устройства, включая:
  - Базы и модули приложений "Лаборатории Касперского".

    Обновления могут быть получены как с Сервера администрирования, так и с серверов обновлений "Лаборатории Касперского". В последнем случае для устройства, являющегося точкой распространения, должна быть создана задача *Загрузка обновлений в хранилища точек* распространения.
  - Обновления приложений сторонних производителей.
  - Инсталляционные пакеты.
  - Обновления Windows, если вы используете Сервер администрирования в роли WSUS-сервера.
- Устанавливать программное обеспечение на другие устройства, в том числе выполнять первоначальное развертывание Агентов администрирования на устройствах.
- Опрашивать сеть с целью обнаружения новых устройств и обновления информации об уже известных устройствах. Точка распространения может использовать те же методы обнаружения устройств, что и Сервер администрирования.

Размещение точек распространения в сети организации преследует следующие цели:

- Уменьшить нагрузку на Сервер администрирования в случае, если источником обновлений служит Сервер администрирования.
- Оптимизировать интернет-трафик, так как в этом случае каждому устройству в сети MSP-клиента не придется обращаться за обновлениями к серверам "Лаборатории Касперского" или к Серверу администрирования.
- Предоставить Серверу администрирования доступ к устройствам за NAT (по отношению к Серверу администрирования) сети MSP-клиента позволяет Серверу администрирования выполнять следующие действия:
  - отправлять уведомления на устройства через UDP в IPv4-сети или IPv6-сети;
  - опрашивать IPv4-сети или IPv6-сети;
  - выполнять первоначальное развертывание;
  - использовать в качестве push-сервера.

Точка распространения назначается на группу администрирования. В этом случае областью действия точки распространения будут устройства, находящиеся в этой группе администрирования и всех ее подгруппах. При этом устройство, выполняющее роль точки распространения, не обязано принадлежать группе администрирования, на которую оно назначено.

Вы можете сделать точку распространения шлюзом соединений. В этом случае устройства, находящиеся в области действия этой точки распространения, будут подключаться к Серверу администрирования не напрямую, а через шлюз. Этот режим полезен в сценариях, когда между устройствами с Агентом администрирования и Сервером администрирования невозможно прямое соединение.

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

Иерархия Серверов администрирования

У MSP может быть более одного Сервера администрирования. Администрировать несколько разрозненных Серверов неудобно, поэтому целесообразно объединять их в иерархию. Взаимодействие "главный – подчиненный" между двумя Серверами администрирования предоставляет следующие возможности:

- Подчиненный Сервер наследует с главного Сервера политики и задачи, устраняется дублирование параметров.
- Выборки устройств на главном Сервере могут включать в себя устройства с подчиненных Серверов.
- Отчеты на главном Сервере могут включать в себя данные (в том числе и детальные) с подчиненных Серверов.

Главный Сервер администрирования получает данные только от невиртуальных подчиненных Серверов администрирования в рамках перечисленных выше параметров. Это ограничение не распространяется на виртуальные Серверы администрирования, которые совместно используют базу данных со своим главным Сервером администрирования.

Виртуальные Серверы администрирования

В рамках физического Сервера администрирования можно создать несколько виртуальных Серверов администрирования, во многом подобных подчиненным Серверам. По сравнению с моделью разделения доступа, основанной на списках контроля доступа (ACL), модель виртуальных Серверов более функциональна и предоставляет большую степень изоляции. В дополнение к структуре групп администрирования, предназначенной для назначения устройствам политик и задач, каждый виртуальный Сервер администрирования имеет собственную группу нераспределенных устройств, собственные наборы отчетов, выборки устройств и события, инсталляционные пакеты, правила перемещения и т. д. Для максимальной взаимной изоляции MSP-клиентов рекомендуется выбирать виртуальные Серверы администрирования, которые будут использоваться для определенных задач. Кроме того, создание виртуального Сервера для каждого MSP-клиента позволяет предоставить клиентам базовые возможности по администрированию своей сети посредством Kaspersky Security Center Web Console.

Виртуальные Серверы во многом подобны подчиненным Серверам администрирования, однако имеют следующие отличия:

- виртуальный Сервер не имеет большинства глобальных параметров и собственных TCP-портов;
- у виртуального Сервера не может быть подчиненных Серверов;
- у виртуального Сервера не может быть собственных виртуальных Серверов;

- на физическом Сервере администрирования видны устройства, группы, события и объекты с управляемых устройств (элементы карантина, реестра приложений и прочее) всех его виртуальных Серверов;
- виртуальный Сервер может сканировать сеть только посредством подключенных к нему точек распространения.

Управление мобильными устройствами с установленным Kaspersky Endpoint Security для Android

Управление мобильными устройствами с установленным приложением Kaspersky Endpoint Security для Android™ (далее KES-устройства) осуществляется с помощью Сервера администрирования. Kaspersky Security Center поддерживает следующие возможности управления KES-устройствами:

- работа с мобильными устройствами как с клиентскими устройствами:
  - членство в группах администрирования;
  - мониторинг, например просмотр статусов, событий и отчетов;
  - изменение локальных параметров и назначение политик для приложения Kaspersky Endpoint Security для Android;
- централизованная отправка команд;
- удаленная установка пакетов мобильных приложений.

Сервер администрирования управляет KES-устройствами по протоколу TLS, TCP-порт 13292.

Развертывание и первоначальная настройка

Kaspersky Security Center является распределенным приложением. В состав Kaspersky Security Center входят следующие приложения:

- Сервер администрирования – центральный компонент, ответственный за управление устройствами организации и хранение данных в СУБД.
- Консоль администрирования – основной инструмент администратора. Консоль администрирования поставляется вместе с Сервером администрирования, но может быть также установлена отдельно на одно или несколько устройств администратора.
- Kaspersky Security Center Web Console – веб-интерфейс Сервера администрирования для выполнения простейших операций. Этот компонент можно установить на любое устройство, удовлетворяющее требованиям к аппаратному и программному обеспечению.
- Агент администрирования – служит для управления установленной на устройстве приложением безопасности, а также для получения информации об устройстве. Агенты администрирования устанавливаются на устройства организации.

Развертывание Kaspersky Security Center в сети организации осуществляется следующим образом:

- установка Сервера администрирования;
- установка Kaspersky Security Center Web Console;
- установка Консоли администрирования на устройстве администратора;
- установка Агента администрирования и приложения безопасности на устройства организации.

Рекомендации по установке Сервера администрирования

В этом разделе содержатся рекомендации, касающиеся установки Сервера администрирования. В разделе также содержатся сценарии использования папки общего доступа на устройстве с Сервером администрирования для развертывания Агента администрирования на клиентских устройствах.

Создание учетных записей для служб Сервера администрирования на отказоустойчивом кластере

По умолчанию инсталлятор самостоятельно создает непривилегированные учетные записи для служб Сервера администрирования. Такое поведение наилучшим образом подходит для установки Сервера администрирования на обычное устройство.

Однако при установке Сервера администрирования на отказоустойчивый кластер следует поступить иначе:

1. Создать непривилегированные доменные учетные записи для служб Сервера администрирования и сделать их членами глобальной доменной группы безопасности KLAdmins.
2. Задать в инсталляторе Сервера администрирования созданные доменные учетные записи для служб.

Выбор СУБД

При выборе СУБД, используемой Сервером администрирования, следует руководствоваться количеством устройств, которые обслуживает Сервер администрирования.

В таблице ниже перечислены допустимые варианты СУБД и рекомендации и ограничения их использования.

СУБД	Рекомендации и ограничения
SQL Server Express Edition 2016 и выше	Используйте эту СУБД, если вы планируете запустить один Сервер администрирования менее чем для 10 000 устройств. Рекомендуется выключить задачу инвентаризации программного обеспечения и выключить (в параметрах политики Kaspersky Endpoint Security) уведомления Сервера администрирования о запуске приложений. Вы можете ограничить максимальное количество событий в хранилище событий, чтобы предотвратить переполнение базы данных. Дополнительную информацию см. в разделе: Расчет места в базе данных. Недопустимо совместное использование СУБД SQL Server Express Edition Сервером администрирования и какого-либо другого приложения. База данных Microsoft SQL Express не поддерживается для задачи **Синхронизация обновлений Windows Update**.
Локальный SQL Server Edition, отличный от Express, 2016 и выше	Нет ограничений.
Удаленный SQL Server Edition, отличный от Express, 2016 и выше	Допустимо только в случае, если оба устройства находятся в одном домене Windows; если домены разные, то между ними должно быть установлено двустороннее отношение доверия.
Локальный или удаленный MySQL 8.0.20 или выше	Используйте эту СУБД, если вы планируете запустить один Сервер администрирования менее чем на 50 000 устройствах. Рекомендуется выключить задачу инвентаризации программного обеспечения и выключить (в параметрах политики Kaspersky Endpoint Security) уведомления Сервера администрирования о запуске приложений. Дополнительную информацию см. в разделе: Расчет места в базе данных.
Локальная или удаленная версия MariaDB (см. поддерживаемые версии)	Используйте эту СУБД, если вы планируете запустить один Сервер администрирования менее чем на 20 000 устройствах. Рекомендуется выключить задачу инвентаризации программного обеспечения и выключить (в параметрах политики Kaspersky Endpoint Security) уведомления Сервера администрирования о запуске приложений. Дополнительную информацию см. в разделе: Расчет места в базе данных.
PostgreSQL, Postgres Pro (см. поддерживаемые версии)	Используйте одну из этих СУБД, если вы планируете использовать один Сервер администрирования менее чем для 50 000 устройств. Рекомендуется выключить задачу инвентаризации программного обеспечения и выключить (в параметрах политики Kaspersky Endpoint Security) уведомления Сервера администрирования о запуске приложений. Дополнительную информацию см. в разделе: Расчет места в базе данных.

Если вы выбрали MSSQL 2019, вам нужно использовать накопительное исправление CU12 или выше. Чтобы избежать ошибки и перегрузки системы, которая может возникнуть.

Если вы используете СУБД PostgreSQL, MariaDB или MySQL, на вкладке **События** может отображаться неполный список событий для выбранного клиентского устройства. Это происходит, когда СУБД хранит очень большое количество событий. Вы можете увеличить количество отображаемых событий, выполнив одно из следующих действий:

- Удалить ненужные события.
- Сократить срок хранения ненужных событий.

Чтобы увидеть полный список событий, зарегистрированных на Сервере администрирования для устройства, используйте Отчеты.

Указание адреса Сервера администрирования

При установке Сервера администрирования необходимо задать внешний адрес Сервера администрирования. Этот адрес по умолчанию используется при создании инсталляционных пакетов Агента администрирования. В дальнейшем адрес Сервера администрирования можно будет изменить средствами Консоли администрирования, однако при этом он не изменится автоматически в уже созданных инсталляционных пакетах Агента администрирования.

Настройка защиты в сети организации-клиента

После завершения инсталляции Сервера администрирования запускается Консоль администрирования, которая предлагает выполнить первоначальную настройку с помощью мастера. Во время работы мастера первоначальной настройки в корневой группе администрирования создаются следующие политики и задачи:

- политика Kaspersky Endpoint Security;
- групповая задача обновления Kaspersky Endpoint Security;
- групповая задача проверки устройства Kaspersky Endpoint Security;
- политика Агента администрирования;
- задача поиска уязвимостей (задача Агента администрирования);
- задача установки обновлений и закрытия уязвимостей (задача Агента администрирования).

Политики и задачи создаются с параметрами по умолчанию, которые могут оказаться неоптимальными или даже непригодными для данной организации. Поэтому следует просмотреть свойства созданных объектов и, в случае необходимости, внести изменения вручную.

В этом разделе содержится информация о ручной настройке политик, задач и других параметров Сервера администрирования, а также информация о точке распространения, построении структуры групп администрирования, иерархии задач и других настройках.

Ручная настройка политики Kaspersky Endpoint Security

Этот раздел содержит рекомендации по настройке параметров политики Kaspersky Endpoint Security, которую создает мастер первоначальной настройки. Вы можете выполнить настройку в окне свойств политики.

При изменении параметра следует помнить, что для того, чтобы значение параметра использовалось на рабочей станции, следует нажать на кнопку с "замком" над параметром.

Настройка политики в разделе Продвинутая защита

Полное описание параметров этого раздела приведено в документации Kaspersky Endpoint Security для Windows.

В разделе **Продвинутая защита** можно настроить использование Kaspersky Security Network для Kaspersky Endpoint Security для Windows. Можно также настроить модули Kaspersky Endpoint Security для Windows, такие как Анализ поведения, Защита от эксплойтов, Предотвращение вторжений и Откат вредоносных действий.

В подразделе **Kaspersky Security Network** рекомендуется включить параметр **Kaspersky Security Network**. Использование этого параметра поможет перераспределить и оптимизировать трафик сети. Если параметр **Kaspersky Security Network** выключен, вы можете включить прямое использование серверов KSN.

Настройка политики в разделе Базовая защита

Полное описание параметров этого раздела приведено в документации Kaspersky Endpoint Security для Windows.

В разделе **Базовая защита** окна свойств политики рекомендуется указать дополнительные параметры в подразделах **Сетевой экран** и **Защита от файловых угроз**.

Подраздел **Сетевой экран** содержит параметры, позволяющие контролировать сетевую активность приложений на клиентских устройствах. Клиентское устройство использует сеть, которой присвоен один из следующих статусов: общедоступная, локальная или доверенная. В зависимости от состояния сети Kaspersky Endpoint Security может разрешить или запретить сетевую активность на устройстве. Когда вы добавляете новую сеть в свою организацию, вам нужно присвоить ей соответствующий сетевой статус. Например, если клиентским устройством является ноутбук, рекомендуется, чтобы это устройство использовало общедоступную или доверенную сеть, так как ноутбук не всегда подключен к локальной сети. В подразделе **Сетевой экран** можно проверить, правильно ли вы присвоили статусы используемым в вашей организации сетям.

Чтобы проверить список сетей:

1. В свойствах политики перейдите в раздел **Базовая защита** → **Сетевой экран**.
2. В блоке **Доступные сети** нажмите на кнопку **Настройки**.
3. В открывшемся окне **Сетевой экран** перейдите на вкладку **Сети** для просмотра списка сетей.

В подразделе **Защита от файловых угроз** можно отключить проверку сетевых дисков. Проверка сетевых дисков может создавать значительную нагрузку на сетевые диски. Целесообразнее осуществлять проверку непосредственно на файловых серверах.

Чтобы выключить проверку сетевых дисков:

1. В свойствах политики перейдите в раздел **Базовая защита → Защита от файловых угроз**.
2. В блоке **Уровень безопасности** нажмите на кнопку **Настройки**.
3. В открывшемся окне **Защита от файловых угроз** на вкладке **Общие** снимите флажок **Все сетевые диски**.

Настройка политики в разделе Дополнительные параметры

Полное описание параметров этого раздела приведено в документации Kaspersky Endpoint Security.

Ниже описаны действия по дополнительной настройке, которые рекомендуется выполнить в окне свойств политики Kaspersky Endpoint Security в разделе **Общие параметры**.

Раздел Дополнительные параметры, подраздел Отчеты и хранилища

В разделе **Передача данных на Сервер администрирования**, обратите внимание на флажок **О запускаемых приложениях**. Если этот флажок установлен, в базе данных Сервера администрирования сохраняется информация о всех версиях всех модулей приложений на устройствах в сети организации. Указанная информация может занимать значительный объем в базе данных Kaspersky Security Center (десятки гигабайтов). Поэтому, если в политике верхнего уровня по-прежнему установлен флажок **О запускаемых приложениях**, его необходимо снять.

Раздел Дополнительные параметры, подраздел Интерфейс

Если управление защитой от угроз в сети организации необходимо выполнять централизованно через Консоль администрирования, нужно выключить отображение пользовательского интерфейса Kaspersky Endpoint Security на рабочих станциях (сняв флажок **Отображать интерфейс приложения** в разделе **Взаимодействие с пользователем**) и включить защиту паролем (установив **флажок Включить защиту паролем** в разделе **Защита паролем**).

Настройка политики в разделе Настройка событий

В разделе **Настройка событий** следует выключить сохранение на Сервере администрирования всех событий, за исключением перечисленных ниже:

- На вкладке **Критическое**:
  - *Автозапуск приложения выключен*
  - *Доступ запрещен*
  - *Запуск приложения запрещен*
  - *Лечение невозможно*
  - *Нарушено Лицензионное соглашение*
  - *Не удалось загрузить модуль шифрования*

- *Невозможен запуск двух задач одновременно*
- *Обнаружена активная угроза. Требуется запуск процедуры лечения активного заражения*
- *Обнаружена сетевая атака*
- *Обновлены не все компоненты*
- *Ошибка активации*
- *Ошибка активации портативного режима*
- *Ошибка взаимодействия с Kaspersky Security Center*
- *Ошибка деактивации портативного режима*
- *Ошибка изменения состава компонентов приложения*
- *Ошибка применения правил шифрования / расшифровки файлов*
- *Политика не может быть применена*
- *Процесс завершен*
- *Сетевая активность запрещена*

- На вкладке **Отказ функционирования**: *Ошибка в настройках задачи. Настройки задачи не применены*
- На вкладке **Предупреждение**:
  - *Самозащита приложения выключена*
  - *Некорректный резервный ключ*
  - *Пользователь отказался от политики шифрования*
- На вкладке **Информационное сообщение**: *Запуск приложения запрещен в тестовом режиме.*

Ручная настройка групповой задачи обновления Kaspersky Endpoint Security

Если источником обновлений является Сервер администрирования, то для групповых задач обновления Kaspersky Endpoint Security оптимальным и рекомендуемым является расписание **При загрузке обновлений в хранилище** при установленном флажке **Использовать автоматическое определение случайного интервала между запусками задачи**.

Если для каждой точки распространения будет создана локальная задача загрузки обновлений в хранилище с серверов "Лаборатории Касперского", то для групповой задачи обновления Kaspersky Endpoint Security оптимальным и рекомендуемым будет периодический запуск по расписанию. Значение периода автономизации следует в этом случае установить в 1 час.

Ручная настройка групповой задачи проверки устройства Kaspersky Endpoint Security

Мастер первоначальной настройки создает групповую задачу проверки устройства. По умолчанию для задачи выбрано расписание **Запускать по пятницам в 19:00** с автоматической рандомизацией и снят флажок **Запускать пропущенные задачи**.

Это означает, что если устройства организации выключаются по пятницам, например, в 18:30, то задача проверки устройства никогда не будет запущена. Следует настроить оптимальное расписание этой задачи исходя из принятого в организации регламента работы.

Настройка расписания задачи Поиск уязвимостей и требуемых обновлений.

Мастер первоначальной настройки создает для Агента администрирования групповую задачу *Поиск уязвимостей и требуемых обновлений*. По умолчанию для задачи выбрано расписание **Запускать по вторникам в 19:00** с автоматической рандомизацией и установлен флажок **Запускать пропущенные задачи**.

Если регламент работы организации предусматривает выключение устройств в это время, то задача *Поиск уязвимостей и требуемых обновлений* будет запущена после включения устройства (в среду утром). Такое поведение может быть нежелательным, так как поиск уязвимостей может вызывать повышенную нагрузку на процессор и дисковую подсистему устройства. Следует настроить оптимальное расписание задачи исходя из принятого в организации регламента работы.

Ручная настройка групповой задачи установки обновлений и закрытия уязвимостей

Мастер первоначальной настройки создает для Агента администрирования групповую задачу установки обновлений и поиска уязвимостей. По умолчанию настроен запуск задачи ежедневно в 1:00 с автоматической рандомизацией, параметр **Запускать пропущенные задачи** выключен.

Если регламент работы организации предусматривает отключение устройств на ночь, то задача установки обновлений никогда не будет запущена. Следует задать оптимальное расписание задачи поиска уязвимостей исходя из принятого в организации регламента работы. Кроме того, следует учитывать, что в результате установки обновлений может потребоваться перезагрузка устройства.

Построение структуры групп администрирования и назначение точек распространения

Структура групп администрирования в Kaspersky Security Center выполняет следующие функции:

- Задание области действия политик.

  Существует альтернативный способ применения нужных наборов параметров на устройствах с помощью профилей политик. В этом случае область действия политик задается, например, с помощью тегов, местоположения устройств в подразделениях Active Directory и членства в группах безопасности Active Directory.

- Задание области действия групповых задач.

  Существует подход к заданию области действия групповых задач, не основанный на иерархии групп администрирования: использование задач для выборок устройств и наборов устройств.

- Задание прав доступа к устройствам, виртуальным и подчиненным Серверам администрирования.

- Назначение точек распространения.

При построении структуры групп администрирования следует учитывать топологию сети организации для оптимального назначения точек распространения. Оптимальное распределение точек распространения позволяет уменьшить сетевой трафик внутри сети организации.

В зависимости от организационной структуры MSP-клиента и топологии сетей можно выделить следующие типовые конфигурации структуры групп администрирования:

- Один офис.

- Множество небольших изолированных офисов.

Типовая конфигурация MSP-клиента: один офис

В типовой конфигурации "один офис" все устройства находятся в сети организации и "видят" друг друга. Сеть организации может состоять из нескольких выделенных частей (сетей или сегментов сети), связанных узкими каналами.

Возможны следующие способы построения структуры групп администрирования:

- Построение структуры групп администрирования с учетом топологии сети. Структура групп администрирования не обязательно должна точно отражать топологию сети. Достаточно того, чтобы выделенным частям сети соответствовали какие-либо группы администрирования. Можно использовать автоматическое назначение точек распространения, либо назначать точки распространения вручную.

- Построение структуры групп администрирования, не отражающей топологию сети. В этом случае следует отключить автоматическое назначение точек распространения и в каждой выделенной части сети назначить одно или несколько устройств точками распространения на корневую группу администрирования, например на группу **Управляемые устройства**. Все точки распространения окажутся на одном уровне и будут иметь одинаковую область действия "все устройства сети организации". Каждый Агент администрирования будет подключаться к той точке распространения, маршрут к которой является самым коротким. Маршрут к точке распространения можно определить с помощью утилиты tracert.

Типовая конфигурация MSP-клиента: множество небольших изолированных офисов

Этой типовой конфигурации соответствует множество небольших удаленных офисов, возможно, связанных с главным офисом через интернет. Каждый из удаленных офисов находится за NAT, то есть подключение из одного удаленного офиса в другой невозможно – офисы изолированы друг от друга.

Конфигурацию следует обязательно отразить в структуре групп администрирования: для каждого из удаленных офисов следует создать отдельную группу администрирования (группы **Офис 1**, **Офис 2** на рисунке ниже).



Удаленные офисы отражены в структуре групп администрирования

На каждую группу администрирования, соответствующую офису, нужно назначить одну или несколько точек распространения. Точками распространения нужно назначать устройства удаленного офиса, имеющие достаточно места на диске. Устройства, размещенные, например, в группе **Офис 1**, будут обращаться к точкам распространения, назначенным на группу администрирования **Офис 1**.

Если некоторые пользователи физически перемещаются между офисами с ноутбуками, нужно в каждом удаленном офисе дополнительно к упомянутым выше точкам распространения выбрать два и или более устройств и назначить их точками распространения на группу администрирования верхнего уровня (группа **Корневая группа для офисов** на рисунке выше).

Ноутбук, находившийся в группе администрирования **Офис 1**, но физически перемещенный в офис, соответствующий группе **Офис 2**. После перемещения Агент администрирования на ноутбуке попытается обратиться к точкам распространения, назначенным на группу **Офис 1**, но эти точки распространения окажутся недоступны. Тогда Агент администрирования начнет обращаться к точкам распространения, назначенным на группу **Корневая группа для офисов**. Так как удаленные офисы изолированы друг от друга, то из всех точек распространения, назначенных на группу администрирования **Корневая группа для офисов**, успешными будут лишь обращения к точкам распространения, назначенным на группу **Офис 2**. То есть ноутбук, оставаясь в группе администрирования, соответствующей своему исходному офису, будет, тем не менее, использовать точку распространения того офиса, в котором в данный момент находится физически.

Иерархия политик, использование профилей политик

В этом разделе содержится информация об особенностях применения политик к устройствам в группах администрирования. В этом разделе также содержится информация о профилях политик.

Иерархия политик

В Kaspersky Security Center политики предназначены для задания одинакового набора параметров на множестве устройств. Например, областью действия политики приложения P, определенной для группы G, являются управляемые устройства с установленным приложением P, размещенные в группе администрирования G и всех ее подгруппах, исключая те подгруппы, в свойствах которых снят флажок **Наследовать из родительской группы**.

Политика отличается от локальных параметров наличием "замков" (🔒) возле содержащихся в ней параметров. Установленный замок в свойствах политики означает, что соответствующий ему параметр (или группа параметров) должен, во-первых, быть использован при формировании эффективных параметров, во-вторых, должен быть записан в нижележащую политику.

Формирование на устройстве действующих параметров можно представить следующим образом: из политики берутся значения параметров с неустановленным замком, затем поверх них записываются значения локальных параметров, затем поверх полученных значений записываются взятые из политики значения параметров с установленным замком.

Политики одного и того же приложения действуют друг на друга по иерархии групп администрирования: параметры с установленным замком из вышележащей политики переписывают одноименные параметры из нижележащей политики.

Существует особый вид политики – политика для автономных пользователей. Эта политика вступает в силу на устройстве, когда устройство переходит в автономный режим. Политики для автономных пользователей не действуют по иерархии групп администрирования на другие политики.

Профили политик

Применение политик к устройствам, исходя только из иерархии групп администрирования, во многих случаях неудобно. Может возникнуть необходимость создать несколько копий политики для разных групп администрирования и в дальнейшем вручную синхронизировать содержимое этих политик.

Чтобы помочь избежать подобных проблем, Kaspersky Security Center поддерживает *профили политик*. Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на клиентском устройстве (компьютере, мобильном устройстве). При активации профиля изменяются параметры политики, действовавшие на устройстве до активации профиля. Эти параметры принимают значения, указанные в профиле.

Профили политик сейчас имеют следующие ограничения:

- в политике может быть не более 100 профилей;
- профиль политики не может содержать другие профили;
- профиль политики не может содержать параметры уведомлений.

Состав профиля

Профиль политики содержит следующие составные части:

- Имя. Профили с одинаковыми именами действуют друг на друга по иерархии групп администрирования с общим правилами.
- Подмножество параметров политики. В отличие от политики, где содержатся все параметры, в профиле присутствуют лишь те параметры, которые действительно нужны (на которых установлен замок).

- Условие активации – логическое выражение над свойствами устройства. Профиль активен (дополняет политику), только когда условие активации профиля становится истинным. В остальных случаях профиль неактивен и игнорируется. В логическом выражении могут участвовать следующие свойства устройства:
  - состояние автономного режима;
  - свойства сетевого окружения – имя активного правила подключения Агента администрирования;
  - наличие или отсутствие у устройства указанных тегов;
  - местоположение устройства в подразделении Active Directory: явное (устройство находится непосредственно в указанном подразделении) или неявное (устройство находится в подразделении, которое находится внутри указанного подразделения на любом уровне вложенности);
  - членство устройства в группе безопасности Active Directory (явное или неявное);
  - членство владельца устройства в группе безопасности Active Directory (явное или неявное).
- Флажок отключения профиля. Выключенные профили всегда игнорируются, условия их активации не проверяются.
- Приоритет профиля. Условия активации профилей независимы, поэтому одновременно могут активироваться сразу несколько профилей. Если активные профили содержат непересекающиеся наборы параметров, то никаких проблем не возникает. Но если два активных профиля содержат разные значения одного и того же параметра, возникает неоднозначность. Значение неоднозначной переменной будет взято из профиля с большим приоритетом (из того профиля, который располагается выше в списке профилей).

Поведение профилей при действии политик друг на друга по иерархии

Одноименные профили объединяются согласно правилам объединения политик. Профили верхней политики приоритетнее профилей нижней политики. Если в "верхней" политике запрещено изменение параметров (кнопка замок нажата), в "нижней" политике используются условия активации профиля из "верхней" политики. Если в "верхней" политике разрешено изменение параметров, то используются условия активации профиля из "нижней" политики.

Поскольку профиль политики может в условии активации содержать свойство **Устройство в автономном режиме**, профили полностью заменяют функциональность политик для автономных пользователей, которая в дальнейшем не будет поддерживаться.

Политика для автономных пользователей может содержать профили, но активация ее профилей может произойти не ранее, чем устройство перейдет в автономный режим.

Tasks

Kaspersky Security Center управляет работой приложений безопасности "Лаборатории Касперского", установленных на устройствах, путем создания и запуска *задач*. С помощью задач выполняются установка, запуск и остановка приложений, проверка файлов, обновление баз и модулей приложений, другие действия с приложениями.

Вы можете создать задачу для приложения, только если для этого приложения установлен плагин управления.

Задачи могут выполняться на Сервере администрирования и на устройствах.

Задачи, которые выполняются на Сервере администрирования:

- автоматическая рассылка отчетов;
- загрузка обновлений в хранилище Сервера администрирования;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных;
- синхронизация обновлений Windows Update;
- создание инсталляционного пакета на основе образа операционной системы эталонного устройства.

На устройствах выполняются следующие типы задач:

- *Локальные задачи* – это задачи, которые выполняются на конкретном устройстве.

  Локальные задачи могут быть изменены не только администратором средствами Консоли администрирования, но и пользователем удаленного устройства (например, в интерфейсе приложения безопасности). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором, как более приоритетные.

- *Групповые задачи* – это задачи, которые выполняются на всех устройствах указанной группы.

  Если иное не указано в свойствах задачи, групповая задача также распространяется на подгруппы указанной группы. Групповые задачи также действуют (опционально) и на устройства, подключенные к подчиненным и виртуальным Серверам администрирования, размещенным в этой группе и подгруппах.

- *Глобальные задачи* – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.

Для каждого приложения вы можете создавать любое количество групповых задач, глобальных задач и локальных задач.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

Запуск задач на устройстве выполняется только в том случае, если запущено приложение, для которого созданы эти задачи.

Результаты выполнения задач сохраняются в журналах событий Microsoft Windows и Kaspersky Security Center как централизованно на Сервере администрирования, так и локально на каждом устройстве.

Не используйте в параметрах задач конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

Правила перемещения устройств

Размещение устройств в группах администрирования на виртуальном сервере, соответствующем MSP-клиенту, целесообразно автоматизировать при помощи *правил перемещения устройств*. Правило перемещения состоит из трех основных частей: имени, условия выполнения (логического выражения над атрибутами устройства) и целевой группы администрирования. Правило перемещает устройство в целевую группу администрирования, если атрибуты устройства удовлетворяют условию выполнения правила.

Правила перемещения устройств имеют приоритеты. Сервер администрирования проверяет атрибуты устройства на соответствие условию выполнения каждого правила, в порядке убывания приоритета правил. Если атрибуты устройства удовлетворяют условию выполнения правила, то устройство перемещается в целевую группу, и на этом обработка правил для этого устройства прекращается. Если атрибуты устройства удовлетворяют сразу нескольким правилам, то устройство будет перемещено в целевую группу того правила, которое имеет больший приоритет (стоит в списке правил выше).

Правила перемещения устройств могут создаваться неявно. Например, в свойствах пакета или задачи удаленной установки может быть указана группа администрирования, в которую должно попасть устройство после установки на нем Агента администрирования. Также правила перемещения могут быть созданы администратором Kaspersky Security Center в явном виде, в списке правил перемещения. Список расположен в Консоли администрирования в свойствах группы **Нераспределенные устройства**.

Правило перемещения по умолчанию предназначено для однократного первоначального размещения устройств в группах администрирования. Правило перемещает только один раз устройства, находящиеся в группе **Нераспределенные устройства**. Если устройство однажды было перемещено этим правилом, правило не переместит его повторно, даже если вернуть устройство вручную в группу **Нераспределенные устройства**. Это рекомендуемый способ использования правил перемещения.

Можно перемещать устройства, уже размещенные в группах администрирования. Для этого в свойствах правила нужно снять флажок **Перемещать только устройства, не размещенные в группах администрирования**.

Наличие правил перемещения, действующих на устройства, уже размещенные в группах администрирования, существенно увеличивает нагрузку на Сервер администрирования.

Можно создать правило перемещения, способное многократно действовать на одно и то же устройство.

Настоятельно рекомендуется избегать подхода к работе с управляемыми устройствами, при котором одно и то же устройство многократно перемещается из группы в группу, например, с целью применения к устройству особой политики, запуска специальной групповой задачи, обновления с определенной точки распространения.

Подобные сценарии не поддерживаются, так как они крайне неэффективны по нагрузке на Сервер администрирования и на сетевой трафик. Также эти сценарии противоречат модели работы Kaspersky Security Center (особенно в области прав доступа, событий и отчетов). Следует искать другое решение, например, использовать профили политик, задачи для выборок устройств, назначать Агенты администрирования согласно методике и так далее.

Категоризация программного обеспечения

Основным средством контроля запуска приложений являются *категории "Лаборатории Касперского"* (далее также *KL-категории*). KL-категории облегчают администратору Kaspersky Security Center работу по поддержанию категоризации ПО и минимизируют объем трафика, передаваемого на управляемые устройства.

Пользовательские категории следует создавать только для приложений, не подпадающих ни под одну KL-категорию (например, для приложений, разработанных на заказ). Пользовательские категории создаются на основе дистрибутива приложения (MSI) или на основе папки с дистрибутивами.

Если имеется большая пополняемая коллекция программного обеспечения, не категоризированного при помощи KL-категорий, может быть целесообразным создать автоматически обновляемую категорию. Такая категория будет автоматически пополняться контрольными суммами исполняемых файлов при изменении папки с дистрибутивами.

Не создавайте автоматически обновляемые категории программного обеспечения для папок Мои документы, %windir%, %ProgramFiles% и %ProgramFiles(x86)%. Файлы в этих папках часто меняются, что приводит к увеличению нагрузки на Сервер администрирования и к увеличению трафика в сети. Следует создать отдельную папку с коллекцией программного обеспечения и время от времени пополнять ее.

О мультитенантных приложениях

Kaspersky Security Center позволяет администраторам поставщиков услуг и администраторам тенантов использовать приложения "Лаборатории Касперского" с поддержкой мультитенантности. После установки мультитенантного приложения "Лаборатории Касперского" в инфраструктуре поставщика услуг, тенанты могут начать использовать приложение.

Чтобы разделить задачи и политики, относящиеся к разным тенантам, вам нужно создать отдельный виртуальный Сервер администрирования в Kaspersky Security Center для каждого тенанта. Все задачи и политики для мультитенантных приложений, выполняемых для тенанта, должны быть созданы для группы администрирования Управляемые устройства виртуального Сервера администрирования, соответствующей этому тенанту. Задачи, созданные для групп администрирования, относящихся к главному Серверу администрирования, не влияют на устройства тенантов.

В отличие от администраторов поставщиков услуг, администратор тенанта может создавать и просматривать задачи и политики приложений только для устройств соответствующего тенанта. Наборы задач и параметров политик, доступные администраторам поставщика услуг и администраторам тенантов, различаются. Некоторые задачи и некоторые параметры политики недоступны для администраторов тенантов.

Внутри иерархической структуры тенанта политики, созданные для мультитенантных приложений, наследуются как для групп администрирования более низкого уровня, так и для групп администрирования верхнего уровня: политика распространяется на все клиентские устройства, принадлежащие тенанту.

Резервное копирование и восстановление параметров Сервера администрирования

Для резервного копирования параметров Сервера администрирования и используемой им базы данных предусмотрены задача резервного копирования и утилита klbackup. Резервная копия включает в себя все основные параметры и объекты Сервера администрирования: сертификаты Сервера администрирования, мастер-ключи шифрования дисков управляемых устройств, ключи для лицензий, структуру групп администрирования со всем содержимым, задачи, политики и так далее. Имея резервную копию, можно восстановить работу Сервера администрирования в кратчайшие сроки – от десятков минут до двух часов.

В случае отсутствия резервной копии сбой может привести к безвозвратной потере сертификатов и всех параметров Сервера администрирования. Это повлечет необходимость заново настраивать Kaspersky Security Center, а также заново выполнять первоначальное развертывание Агента администрирования в сети организации. Кроме того, будут потеряны и мастер-ключи шифрования дисков управляемых устройств, что создаст риск безвозвратной потери зашифрованных данных на устройствах с Kaspersky Endpoint Security. Поэтому не следует отказываться от регулярного создания резервных копий Сервера администрирования с помощью штатной задачи резервного копирования.

Мастер первоначальной настройки приложения создает задачу резервного копирования параметров Сервера администрирования с ежедневным запуском в четыре часа ночи. Резервные копии по умолчанию сохраняются в папке %ALLUSERSPROFILE%\Application Data\KasperskySC.

Если в качестве СУБД используется экземпляр Microsoft SQL Server, установленный на другом устройстве, следует изменить задачу резервного копирования: указать в качестве папки для хранения сделанных резервных копий UNC-путь, доступный на запись как службе Сервера администрирования, так и службе SQL Server. Это требование является следствием особенности резервного копирования в СУБД Microsoft SQL Server.

Если в качестве СУБД используется локальный экземпляр Microsoft SQL Server, также рекомендуется сохранять резервные копии на отдельном носителе, чтобы обезопасить их от повреждения одновременно с Сервером администрирования.

Поскольку резервная копия содержит важные данные, в задаче резервного копирования и в утилите klbackup предусмотрена защита резервных копий паролем. По умолчанию задача резервного копирования создается с пустым паролем. Следует обязательно задать пароль в свойствах задачи резервного копирования. Несоблюдение этого требования приведет к тому, что ключи сертификатов Сервера администрирования, ключи для лицензий и мастер-ключи шифрования дисков управляемых устройств окажутся незашифрованными.

Помимо регулярного резервного копирования, следует также создавать резервную копию перед всеми значимыми изменениями, в том числе перед обновлением Сервера администрирования до новой версии и перед установкой патчей Сервера администрирования.

Если вы используете Microsoft SQL Server в качестве СУБД, вы можете минимизировать размер резервных копий. Для этого установите флажок **Сжимать резервные копии (Compress backup)** в параметрах SQL Server.

Восстановление из резервной копии выполняется с помощью утилиты klbackup на только что установленном и работоспособном экземпляре Сервера администрирования той версии, для которой была сделана резервная копия (или более новой).

Экземпляр Сервера администрирования, на который выполняется восстановление, должен использовать СУБД того же типа (например, тот же SQL Server или MariaDB) той же самой или более новой версии. Версия Сервера администрирования может быть той же самой (с аналогичным или более новым патчем) или более новой.

В этом разделе описаны типовые сценарии восстановления параметров и объектов Сервера администрирования.

Вышло из строя устройство с Сервером администрирования

Если в результате сбоя вышло из строя устройство с Сервером администрирования, рекомендуется выполнить следующие действия:

- Новому Серверу назначить тот же самый адрес: NetBIOS-имя, FQDN-имя, статический IP – в зависимости от того, что было задано при развертывании Агентов администрирования.
- Установить Сервер администрирования с использованием СУБД того же типа, той же или более новой версии. Можно установить ту же версию Сервера с тем же или более новым патчем, или более новую версию. После установки не следует выполнять первоначальную настройку с помощью мастера.
- Из меню **Пуск** запустить утилиту резервного копирования klbackup и выполнить восстановление.

Повреждены параметры Сервера администрирования или база данных

Если Сервер администрирования стал неработоспособен в результате повреждения параметров или базы данных (например, из-за сбоя питания), рекомендуется использовать следующий сценарий восстановления:

1. Выполнить проверку файловой системы на пострадавшем устройстве.
2. Деинсталлировать неработоспособную версию Сервера администрирования.
3. Заново установить Сервер администрирования с использованием СУБД того же типа, той же или более новой версии. Можно установить ту же версию Сервера с тем же или более новым патчем, или более новую версию. После установки не следует выполнять первоначальную настройку с помощью мастера.
4. Из меню **Пуск** запустить утилиту резервного копирования klbackup и выполнить восстановление.

Недопустимо восстанавливать Сервер администрирования любым другим способом, кроме штатной утилиты klbackup.

Во всех случаях восстановления Сервера с помощью стороннего программного обеспечения неизбежно произойдет рассинхронизация данных на узлах распределенного приложения Kaspersky Security Center и, как следствие, неправильная работа приложения.

Развертывание Агента администрирования и приложения безопасности

Для управления устройствами организации требуется установить на устройства Агент администрирования. Развертывание распределенного приложения Kaspersky Security Center на устройствах организации обычно начинается с установки на них Агента администрирования.

В Microsoft Windows XP Агент администрирования может некорректно выполнять следующие операции: загрузка обновлений напрямую с серверов "Лаборатории Касперского" (если выполняет роль точки распространения); функционирование в качестве прокси-сервера KSN (если выполняет роль точки распространения); и обнаружение уязвимостей приложений сторонних производителей (при использовании Системного администрирования).

Первоначальное развертывание

Если на устройстве уже установлен Агент администрирования, удаленная установка приложений на такое устройство осуществляется с помощью самого Агента администрирования. При этом передача дистрибутива устанавливаемого приложения вместе с заданными администратором инсталляционными параметрами осуществляется по каналам связи между Агентами администрирования и Сервером администрирования. Для передачи дистрибутива можно использовать промежуточные центры распространения в виде точек распространения, многоадресную рассылку и прочие средства. Подробные сведения об установке приложений на управляемые устройства, на которых уже установлен Агент администрирования, см. далее в этом разделе.

Первоначальную установку Агента администрирования на устройства на платформе Microsoft Windows можно осуществлять следующими способами:

- С помощью сторонних средств удаленной установки приложений.
- С помощью групповых политик Windows: использование стандартных средств управления Windows для групповых политик.
- Принудительно с помощью соответствующих параметров в задаче удаленной установки приложения Kaspersky Security Center.
- Путем рассылки пользователям устройств ссылок на автономные пакеты, сформированные Kaspersky Security Center. Автономные пакеты представляют собой исполняемые модули, содержащие в себе дистрибутивы выбранных приложений с настроенными параметрами.
- Вручную, запуская инсталляторы приложений на устройствах.

На платформах, отличных от Microsoft Windows, первоначальную установку Агента администрирования на управляемых устройствах следует осуществлять имеющимися сторонними средствами либо вручную путем отправки пользователям архива с предварительно сконфигурированным дистрибутивом. Обновлять Агент администрирования до новой версии, а также устанавливать другие приложения "Лаборатории Касперского" на этих платформах можно с помощью задач удаленной установки приложений, используя уже имеющиеся на устройствах Агенты администрирования. Установка в этом случае происходит аналогично установке на платформе Microsoft Windows.

Выбирая способ и стратегию развертывания приложений в управляемой сети, следует принимать во внимание ряд факторов (неполный список):

- конфигурацию сети организации;
- общего количества устройств;
- наличие доменов Windows в управляемой сети, возможность внесения изменений в групповые политики Active Directory в таких доменах;
- знание учетной записи (записей) с правами локального администратора на тех устройствах, где предстоит провести первоначальное развертывание приложений "Лаборатории Касперского" (то есть доступность доменной учетной записи с правами локального администратора либо наличие унифицированных локальных учетных записей с административными правами на таких устройствах);
- характер связи и ширину сетевых каналов между Сервером администрирования и сетями MSP-клиентов и ширину сетевых каналов внутри этих сетей;
- используемые на момент начала развертывания параметры безопасности на удаленных устройствах (в частности, использование UAC и режима Simple File Sharing).

Настройка параметров инсталляторов

Прежде чем приступать к развертыванию в сети приложений "Лаборатории Касперского", следует определить параметры инсталляции – те параметры, которые настраиваются в ходе установки приложения. При установке Агента администрирования требуется задать, по крайней мере, адрес для подключения к Серверу администрирования, параметры proxy, а возможно, и некоторые дополнительные параметры. В зависимости от выбранного способа установки параметры можно задавать различными способами. В простейшем случае (при интерактивной установке вручную на выбранное устройство) необходимые параметры можно задать с помощью пользовательского интерфейса инсталлятора, так что в некоторых случаях первоначальное развертывание может даже осуществляться путем отправки пользователям ссылки на дистрибутив Агента администрирования с указанием параметров (адреса Сервера администрирования и тому подобное), которые пользователь должен будет ввести в интерфейсе инсталлятора.

Этот способ настройки параметров не рекомендуется к использованию на практике ввиду неудобства для пользователей и высокой вероятности ошибок при ручном задании ими параметров и не подходит для тихой установки приложений на группы устройств. В типичном случае администратор должен централизованно указать значения параметров, которые в дальнейшем могут быть использованы для формирования автономных пакетов. Автономные пакеты являются самораспаковывающимися архивами дистрибутивов с заданными администратором параметрами. Автономные пакеты могут быть расположены на ресурсах, доступных для загрузки конечными пользователями (например, на Веб-сервере Kaspersky Security Center) и для тихой установки на выбранные устройства в сети.

Инсталляционные пакеты

Первый и основной способ настройки инсталляционных параметров приложений является универсальным и подходит для всех способов установки приложений: как средствами Kaspersky Security Center, так и с помощью большинства сторонних средств. Этот способ подразумевает создание в Kaspersky Security Center инсталляционных пакетов приложений.

Инсталляционные пакеты создаются следующими способами:

- автоматически из указанных дистрибутивов на основании входящих в их состав *описателей* (файлов с расширением kud, содержащих правила установки и анализа результата и другую информацию);

- из исполняемых файлов инсталляторов или инсталляторов в формате Microsoft Windows Installer (MSI) – для стандартных или поддерживаемых приложений.

Созданные инсталляционные пакеты представляют собой папки с вложенными подпапками и файлами. Помимо исходного дистрибутива, в состав инсталляционного пакета входят редактируемые параметры (включая параметры самого инсталлятора и правила обработки таких ситуаций, как необходимость перезагрузки операционной системы для завершения инсталляции), а также небольшие вспомогательные модули.

Значения параметров инсталляции, специфичные для конкретного поддерживаемого приложения, можно задавать в пользовательском интерфейсе Консоли администрирования при создании инсталляционного пакета (еще больше параметров для настройки может быть доступно в свойствах уже созданного инсталляционного пакета). В случае удаленной установки приложений средствами Kaspersky Security Center инсталляционные пакеты доставляются на устройства таким образом, что при запуске инсталлятора приложения ему становятся доступны все заданные администратором параметры. При использовании сторонних средств установки приложений "Лаборатории Касперского" достаточно обеспечить доступность на устройстве всего инсталляционного пакета, то есть дистрибутива и его параметров. Инсталляционные пакеты создаются и хранятся Kaspersky Security Center в соответствующей папке каталога общих данных.

Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.

О том, как именно можно воспользоваться этим способом настройки параметров для приложений "Лаборатории Касперского" перед их развертыванием сторонними средствами, см. в разделе "Развертывание с помощью механизма групповых политик Microsoft Windows".

Сразу после установки Kaspersky Security Center автоматически создается несколько инсталляционных пакетов, готовых к установке, в том числе пакеты Агента администрирования и приложения безопасности для платформы Microsoft Windows.

Использование инсталляционных пакетов для развертывания приложений в сети MSP-клиента в ряде случаев подразумевает необходимость создания инсталляционных пакетов на виртуальных Серверах, соответствующих MSP-клиентам. Создание инсталляционных пакетов на виртуальных Серверах позволяет использовать в инсталляционных пакетах для разных MSP-клиентов различные параметры инсталляции. В первую очередь это необходимо в инсталляционных пакетах Агента администрирования, так как Агенты администрирования, развернутые в сетях разных MSP-клиентов, используют различные адреса подключения к Серверу администрирования. Собственно, адрес подключения и определяет, к какому виртуальному Серверу подключается Агент администрирования.

Помимо наличия возможности создания новых инсталляционных пакетов непосредственно на виртуальном Сервере, основным режимом работы с инсталляционными пакетами на виртуальных Серверах является распространение инсталляционных пакетов главного Сервера на виртуальные. Распространять выбранные (или все) пакеты на выбранные виртуальные Серверы (в том числе все Серверы, входящие в выбранную группу администрирования) можно с помощью соответствующей задачи Сервера администрирования. Также при создании нового виртуального Сервера в мастере можно выбрать список инсталляционных пакетов главного Сервера. Выбранные пакеты будут сразу распространены на вновь созданный виртуальный Сервер.

При распространении инсталляционного пакета не происходит полного копирования его содержимого. В файловом хранилище, соответствующем распространенному инсталляционному пакету на виртуальном Сервере, хранятся только файлы параметров, специфичных для данного виртуального Сервера. Основная, неизменная часть инсталляционного пакета (включая сам дистрибутив устанавливаемого приложения) хранится только в хранилище главного Сервера. Это позволяет существенно повысить производительность системы и снизить объем требуемого дискового пространства. При работе с инсталляционными пакетами, распространенными на виртуальные Серверы (то есть при работе задач удаленной установки или при создании автономных инсталляционных пакетов) происходит "сложение" данных из исходного инсталляционного пакета главного Сервера и файлов с параметрами, соответствующих распространенному пакету на виртуальном Сервере.

Несмотря на то, что лицензионный ключ для приложения можно задать в свойствах инсталляционного пакета, желательно не использовать этот способ распространения лицензий, так как файлы в папке можно прочитать, получив доступ случайно. Следует использовать автоматически распространяемые лицензионные ключи или задачи установки для лицензионных ключей.

Свойства MSI и файлы трансформации

Другим способом настроить параметры инсталляции на платформе Windows является задание свойств MSI и файлов трансформации. Этот способ может быть использован при установке с помощью сторонних средств, ориентированных на работу с инсталляторами в формате Microsoft Installer, а также при установке через групповые политики Windows при помощи штатных средств Microsoft или иных сторонних инструментов для работы с групповыми политиками Windows.

Развертывание при помощи сторонних средств удаленной установки приложений

При наличии в организации каких-либо средств удаленной установки приложений (например, Microsoft System Center) целесообразно выполнять первоначальное развертывание при помощи этих средств.

Нужно выполнить следующие действия:

- Выбрать способ настройки параметров инсталляции, наиболее подходящий для используемого средства развертывания.
- Определить механизм синхронизации между изменением параметров инсталляционных пакетов через интерфейс Консоли администрирования и работой выбранных сторонних средств развертывания приложений из данных инсталляционных пакетов.

Общие сведения о задачах удаленной установки приложений Kaspersky Security Center

Kaspersky Security Center предоставляет разнообразные механизмы удаленной установки приложений, реализованные в виде задач удаленной установки приложений. Создать задачу удаленной установки можно как для указанной группы администрирования, так и для набора устройств или для выборки устройств (такие задачи отображаются в Консоли администрирования в папке **Задачи**). При создании задачи можно выбрать инсталляционные пакеты (Агента администрирования и/или другого приложения), подлежащие установке при помощи данной задачи, а также задать ряд параметров, определяющих способ удаленной установки.

Задачи для групп администрирования действуют не только на устройства, принадлежащие этой группе, но и на все устройства всех подгрупп выбранной группы. Если в параметрах задачи включен соответствующий параметр, задача распространяется на устройства подчиненных Серверов администрирования, расположенных в данной группе или ее подгруппах.

Задачи для наборов устройств актуализируют список клиентских устройств при каждом запуске в соответствии с составом выборки устройств на момент запуска задачи. Если в выборке устройств присутствуют устройства, подключенные к подчиненным Серверам администрирования, задача будет запускаться и на этих устройствах.

Для успешной работы задачи удаленной установки на устройствах, подключенных к подчиненным Серверам администрирования, следует при помощи задачи распространения предварительно распространить используемые задачей инсталляционные пакеты на соответствующие подчиненные Серверы администрирования.

Развертывание с помощью механизма групповых политик Microsoft Windows

Первоначальное развертывание Агентов администрирования рекомендуется осуществлять с помощью групповых политик Microsoft Windows при выполнении следующих условий:

- устройства являются членами домена Active Directory;
- разрешен доступ к контроллеру домена с правами администратора, позволяющими создавать и модифицировать групповые политики Active Directory;
- имеется возможность переноса настроенных инсталляционных пакетов в сеть управляемых устройств (в папку общего доступа, доступную на чтение для всех устройств);
- план развертывания позволяет дождаться штатной перезагрузки устройств до начала развертывания на них Агентов администрирования, или к устройствам можно принудительно применить групповую политику Windows.

Суть этого способа развертывания заключается в следующем:

- Дистрибутив приложения в формате Microsoft Installer (MSI-пакет) размещается в папке общего доступа (в папке, к которой имеют доступ на чтение учетные записи LocalSystem устройств).
- В групповой политике Active Directory создается объект установки данного дистрибутива.

- Область действия установки задается привязкой к организационному подразделению и / или к группе безопасности, в которую входят устройства.

- При очередном входе устройства в домен (до входа в систему пользователей устройства) выполняется проверка наличия требуемого приложения среди установленных приложений. Если приложение отсутствует, происходит загрузка дистрибутива с заданного в политике ресурса и его установка.

Одним из преимуществ этого способа развертывания является то, что назначенные приложения устанавливаются на устройства при загрузке операционной системы еще до входа пользователя в систему. Даже если пользователь, имеющий необходимые права, удалит приложение, при следующей загрузке операционной системы оно будет установлено снова. Недостатком этого способа развертывания является то, что произведенные администратором изменения в групповой политике не вступят в силу до перезагрузки устройств (без применения дополнительных средств).

С помощью групповых политик можно устанавливать как Агент администрирования, так и другие приложения, инсталляторы которых имеют формат Windows Installer.

> Установка Агента администрирования из пакета MSI возможна только в тихом режиме. Интерактивная установка Агента из пакета MSI не поддерживается.

При выборе этого способа развертывания, помимо прочего, необходимо оценить нагрузку на файловый ресурс, с которого будет осуществляться копирование файлов на устройства при применении групповой политики Windows. Вам также необходимо выбрать способ доставки настроенного инсталляционного пакета на этот ресурс и метод синхронизации соответствующих изменений в параметрах инсталляционного пакета.

Работа с политиками Microsoft Windows с помощью задачи удаленной установки приложений Kaspersky Security Center

Данный способ развертывания возможен только в том случае, если доступ к контроллеру домена, в который входят устройства, возможен с устройства, где установлен Сервер администрирования, а с устройств доступна для чтения папка общего доступа Сервера администрирования (в которой расположены инсталляционные пакеты). Поэтому данный способ развертывания не рассматривается в контексте MSP.

Самостоятельная установка приложений с помощью политик Microsoft Windows

Администратор может самостоятельно создать в групповой политике Windows объекты, необходимые для установки. В этом случае нужно выложить пакеты на отдельный файловый сервер и сослаться на них.

Возможны следующие сценарии установки:

- Администратор создает инсталляционный пакет и настраивает его свойства в Консоли администрирования. Затем администратор копирует целиком подпапку EXEC этого пакета из папки общего доступа Kaspersky Security Center в папку на специализированном файловом ресурсе организации. Объект групповой политики ссылается MSI-файл этого пакета, лежащего в подпапке на специализированном файловом ресурсе организации.

- Администратор загружает дистрибутив приложения (в том числе дистрибутив Агента администрирования) из интернета и выкладывает его на специализированный файловый ресурс организации. Объект групповой политики ссылается MSI-файл этого пакета, лежащего в подпапке на специализированном файловом ресурсе организации. Настройка параметров инсталляции осуществляется путем настройки свойств MSI или настройкой файлов трансформации MST.

Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center

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 при условии, что на каждом устройстве есть учетные записи пользователей с правами локального администратора.

Принудительная установка может быть использована и в случае, если устройства не доступны Серверу администрирования непосредственно: например, устройства расположены в изолированных сетях, или устройства расположены в локальной сети, а Сервер администрирования – в демилитаризованной зоне.

В случае первоначального развертывания Агент администрирования не устанавливается. Поэтому в параметрах задачи удаленной установки невозможно выбрать распространение файлов, необходимых для установки приложения с помощью Агента администрирования. Вы можете распространять файлы, только используя ресурсы операционной системы с помощью Сервера администрирования или точек распространения.

Служба Сервера администрирования должна запускаться под учетной записью, имеющей права администратора на целевых устройствах. Также вы можете указать учетную запись, имеющую доступ к административным ресурсам общего доступа admin$, в параметрах задачи удаленной установки.

По умолчанию задача удаленной установки подключается к устройствам, используя учетные данные учетной записи, под которой запущен Сервер администрирования, то есть под учетной записью, которая имеет доступ к административным ресурсам общего доступа admin$. Вам нужно указать эту учетную запись в параметрах задачи удаленной установки, только если Агент администрирования не установлен на целевых устройствах.
При создании задачи удаленной установки для запуска на устройствах под управлением Linux вам нужно всегда указывать учетную запись для создания SSH-соединения.

Вы можете указать целевые устройства явно (списком), выбрав группу администрирования Kaspersky Security Center, которой они принадлежат, либо созданием выборки устройств по определенному условию. Время запуска установки определяется расписанием задачи. Если в свойствах задачи включен параметр **Запускать пропущенные задачи**, задача может запускаться сразу при включении устройств или при переносе их в целевую группу администрирования.

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 сервисов. Рассылка инсталляционных пакетов на целевые устройства выполняется с помощью функции Kaspersky Security Center, отвечающей за сетевое взаимодействие. При этом должны выполняться следующие условия:

- Целевые устройства доступны со стороны Сервера администрирования или со стороны точки распространения.
- В сети корректно работает разрешение имен для устройств.
- На целевых устройствах включены административные ресурсы общего доступа admin$.
- На целевых устройствах запущены следующие системные службы:
  - Сервер (LanmanServer).

    По умолчанию эта служба запущена.

- DCOM Server Process Launcher (DcomLaunch).
- RPC Endpoint Mapper (RpcEptMapper).
- Вызов удаленной процедуры (Remote Procedure Call, RpcSs).

- TCP-порт 445 открыт на целевых устройствах для обеспечения удаленного доступа с помощью инструментов Windows.

  TCP 139, UDP 137 и UDP 138 используются старыми протоколами и больше не нужны для текущих приложений.

  На сетевом экране должны быть разрешены динамические исходящие порты доступа для соединения Сервера администрирования и точек распространения с целевыми устройствами.

- В параметрах безопасности политики домена Active Directory разрешено обеспечивать работу NTLM-протокола при развертывании Агента администрирования.
- На целевых устройствах под управлением Microsoft Windows XP режим Simple File Sharing выключен.
- На целевых устройствах настроена модель совместного доступа и безопасности *Классическая – локальные пользователи выполняют аутентификацию самих себя*. Такая модель не может быть *Только гостевой – локальные пользователи выполняют аутентификацию как Гость*.
- Устройства являются членами домена, либо на устройствах заблаговременно созданы унифицированные учетные записи с административными правами.

Чтобы успешно развернуть Агент администрирования или другие приложения на устройстве, не подключенном к домену Active Directory с версией операционной системы Windows Server 2003 и выше, необходимо выключить удаленный UAC на этом устройстве. Удаленный UAC – это одна из причин, по которой учетные записи локальных администраторов не могут получить доступ к admin$, который требуется для принудительного развертывания Агента администрирования и других приложений. Выключение удаленного UAC не влияет на локальный UAC.

При установке на новые устройства, еще не размещенные в группах администрирования Kaspersky Security Center, в свойствах задачи удаленной установки можно задать группу администрирования, в которую устройства будут перемещаться по завершении установки на них Агента администрирования.

При создании групповой задачи необходимо помнить, что групповая задача действует на устройства всех вложенных подгрупп выбранной группы. Поэтому не следует дублировать задачи установки в подгруппах.

Упрощенным способом создания задач для принудительной установки приложений является автоматическая установка. Для этого в свойствах группы администрирования вам нужно открыть список инсталляционных пакетов и выбрать те пакеты, которые должны быть установлены на устройствах этой группы. В результате на всех устройствах этой группы и ее подгрупп будут автоматически установлены выбранные инсталляционные пакеты. Период, в течение которого будут установлены пакеты, зависит от пропускной способности сети и общего количества устройств в сети.

Чтобы снизить нагрузку на Сервер администрирования при распространении инсталляционных пакетов на целевые устройства, вы можете выбрать установку с помощью точек распространения в задаче установки. Следует учитывать, что данный способ установки создает значительную нагрузку на устройства, назначенные точками распространения. Рекомендуется выбирать устройства, соответствующие требованиям для точек распространения. Если вы используете точки распространения, вам нужно убедиться, что они присутствуют в каждой из изолированных подсетей, на которых размещены целевые устройства.

Использование точек распространения в качестве локальных центров установки может быть удобно и для установки на устройства в подсетях, соединенных с Сервером администрирования узким каналом связи при наличии широкого канала связи между устройствами внутри подсети.

Объем свободного места в разделе с папкой %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit должен многократно превосходить суммарный объем дистрибутивов устанавливаемых приложений.

Запуск автономных пакетов, сформированных Kaspersky Security Center

Описанные выше способы первоначального развертывания Агента администрирования и приложений могут быть реализованы не всегда из-за невозможности выполнить все необходимые условия. В таких случаях из подготовленных администратором инсталляционных пакетов с необходимыми параметрами установки средствами Kaspersky Security Center можно создать единый исполняемый файл, который называется *автономным пакетом установки*. Автономный инсталляционный пакет может быть опубликован как на внутреннем Веб-сервере (входящем в состав Kaspersky Security Center), если это имеет смысл (настроен доступ к этому Веб-серверу извне для пользователей устройств), так и на специально развернутом Веб-сервере, входящем в состав Kaspersky Security Center Web Console. Также можно скопировать автономные пакеты на другой Веб-сервер.

При помощи Kaspersky Security Center можно разослать по электронной почте выбранным пользователям ссылку на этот файл в папке общего доступа с просьбой запустить файл (интерактивно или с ключом "тихой" установки "-s"). Автономный инсталляционный пакет можно прикрепить к сообщению электронной почты для пользователей устройств, не имеющих доступа к Веб-серверу. Администратор может также скопировать автономный пакет на внешнее устройство и доставить пакет на нужное устройство с целью его последующего запуска.

Автономный пакет можно создать из пакета Агента администрирования, пакета другого приложения (например, приложения безопасности) или сразу из обоих пакетов. Если автономный пакет создан из Агента администрирования и другого приложения, установка начнется с Агента администрирования.

При создании автономного пакета с Агентом администрирования можно указать группу администрирования, в которую будут автоматически перемещаться новые устройства (ранее не размещенные в группах администрирования) по завершении установки на них Агента администрирования.

Автономные пакеты могут работать интерактивно (по умолчанию), с отображением результата установки входящих в них приложений, или в тихом режиме (при запуске с ключом "-s"). Тихий режим может быть использован для установки из каких-либо скриптов (например, из скриптов, настраиваемых для запуска по завершении развертывания образа операционной системы, и тому подобное). Результат установки в тихом режиме определяется кодом возврата процесса.

Возможности ручной установки приложений

Администраторы или опытные пользователи могут устанавливать приложения вручную в интерактивном режиме. При этом можно использовать как исходные дистрибутивы, так и сформированные из них инсталляционные пакеты, расположенные в папке общего доступа Kaspersky Security Center. Инсталляторы по умолчанию работают в интерактивном режиме, запрашивая у пользователя все необходимые значения параметров. Но при запуске процесса setup.exe из корня инсталляционного пакета с ключом "-s" инсталлятор будет работать в тихом режиме с параметрами, заданными при настройке инсталляционного пакета.

При запуске setup.exe из корня инсталляционного пакета сначала произойдет копирование пакета во временную локальную папку, затем из локальной папки будет запущен инсталлятор приложения.

Удаленная установка приложений на устройства с установленным Агентом администрирования

Если на устройстве установлен работоспособный Агент администрирования, подключенный к главному Серверу администрирования или к одному из его подчиненных Серверов, то на этом устройстве можно обновлять версию Агента администрирования, а также устанавливать, обновлять или удалять с помощью Агента администрирования любые поддерживаемые приложения.

Эта функция включается флажком **С помощью Агента администрирования** в свойствах задачи удаленной установки приложений.

Если флажок установлен, то передача на устройства инсталляционных пакетов с заданными администратором инсталляционными параметрами осуществляется по каналам связи между Агентом администрирования и Сервером администрирования.

Для оптимизации нагрузки на Сервер администрирования и минимизации трафика между Сервером администрирования и устройствами целесообразно назначать в каждой удаленной сети или в каждом широковещательном домене точки распространения (см. разделы "О точках распространения" и "Построение структуры групп администрирования и назначение точек распространения"). В этом случае распространение инсталляционных пакетов и параметров инсталлятора осуществляется с Сервера администрирования на устройства через точки распространения.

Также с использованием точек распространения можно выполнять широковещательную (многоадресную) рассылку инсталляционных пакетов, что позволяет многократно снизить сетевой трафик в ходе развертывания приложений.

При передаче инсталляционных пакетов на устройства по каналам связи между Агентами администрирования и Сервером администрирования подготовленные к передаче инсталляционные пакеты дополнительно кешируются в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. При использовании большого числа различных инсталляционных пакетов большого размера и при большом количестве точек распространения размер этой папки может существенно увеличиваться.

Удалять файлы из папки FTServer вручную невозможно. При удалении исходных инсталляционных пакетов соответствующие данные будут автоматически удаляться и из папки FTServer.

Данные, принимаемые на стороне точек распространения, сохраняются в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp.

Удалять файлы из папки $FTCITmp вручную невозможно. По мере завершения задач, использующих данные из папки, содержимое этой папки будет удаляться автоматически.

Поскольку инсталляционные пакеты распространяются по каналам связи между Сервером администрирования и Агентами администрирования из промежуточного хранилища в оптимизированном для передачи по сети формате, невозможно вносить изменения в инсталляционные пакеты в исходной папке инсталляционного пакета. Такие изменения не будут автоматически учтены Сервером администрирования. Если необходимо изменить вручную файлы инсталляционных пакетов (хотя делать это не рекомендуется), нужно обязательно изменить какие-либо параметры инсталляционного пакета в Консоли администрирования. Изменение параметров инсталляционного пакета в Консоли администрирования заставит Сервер администрирования обновить образ пакета в кеше, подготовленном для передачи на устройства.

Управление перезагрузкой устройств в задаче удаленной установки

Часто для завершения удаленной установки приложений (особенно на платформе Windows) требуется перезагрузка устройства.

Если используется задача удаленной установки приложений Kaspersky Security Center, в мастере создания задачи или в окне свойств созданной задачи (раздел **Перезагрузка операционной системы**) можно выбрать вариант действия при необходимости перезагрузки:

- **Не перезагружать устройство**. В этом случае автоматическая перезагрузка не будет выполнена. Для завершения установки потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки будет сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач установки на серверы и другие устройства, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**. В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения установки. Этот вариант подходит для задач установки на устройства, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**. На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Вариант **Запрашивать у пользователя** наиболее подходит для рабочих станций, пользователи которых должны иметь возможность выбрать наиболее подходящий момент для перезагрузки.

Целесообразность обновления баз в инсталляционном пакете антивирусного приложения

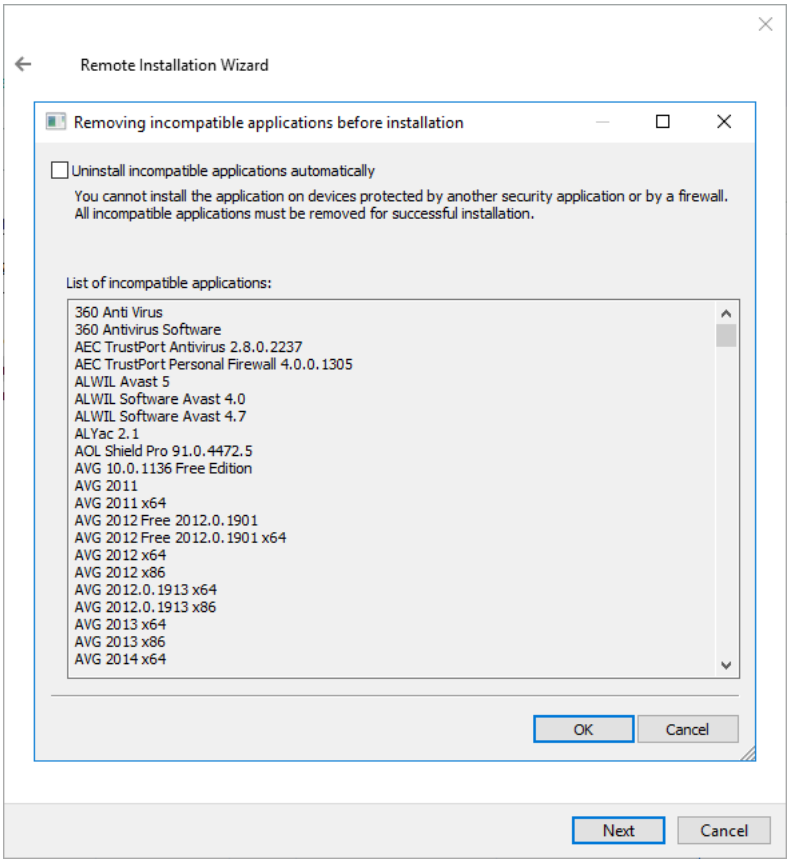
Перед началом развертывания защиты необходимо учитывать возможность обновления антивирусных баз (включая модули автопатчей), распространяемых вместе с дистрибутивом приложения безопасности. Целесообразно перед началом развертывания принудительно обновить базы в составе инсталляционного пакета приложения (например, с помощью соответствующей команды в контекстном меню выбранного инсталляционного пакета). Это уменьшит количество перезагрузок, требующихся для завершения развертывания защиты на устройствах. В случае использования для удаленной установки инсталляционных пакетов, ретранслированных на виртуальные Серверы с главного Сервера, обновлять базы нужно только в самом исходном пакете на главном Сервере. Обновлять базы в ретранслированных пакетах на виртуальных Серверах в этом случае не следует.

Удаление несовместимых приложений безопасности сторонних производителей

Для установки приложений безопасности "Лаборатории Касперского" средствами Kaspersky Security Center может потребоваться удалить стороннее программное обеспечение, несовместимое с устанавливаемым приложением. Существуют два основных способа выполнить эту задачу.

Автоматическое удаление несовместимых приложений с помощью мастера установки

Когда вы запускаете мастер установки, он показывает список приложений, несовместимых с приложением "Лаборатории Касперского":



Список несовместимых приложений, который отображается в мастере удаленной установки

Kaspersky Security Center обнаруживает несовместимое программное обеспечение. Соответственно, вы можете установить флажок **Удалять несовместимые приложения автоматически**, чтобы продолжить установку. Если снять этот флажок и не удалить несовместимое программное обеспечение, произойдет ошибка и приложение "Лаборатории Касперского" не установится.

Автоматическое удаление несовместимых приложений поддерживается различными типами установки.

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.

Удаление Агента администрирования, защищенного паролем, с помощью командной строки

Чтобы удаленно деинсталлировать Агент администрирования, для которого вы установили пароль для удаления, вы можете использовать командную строку.

Если вы потеряли или забыли пароль от Агента администрирования, установленного на устройстве и защищенного паролем, которое больше не находится под управлением Kaspersky Security Center, вы не сможете удалить этот Агент администрирования с помощью утилиты klmover, средствами Cleaner (cleaner.exe) или с помощью командной строки. В этом случае необходимо переустановить операционную систему на устройстве с установленным Агентом администрирования, защищенным паролем.

Чтобы удалить Агент администрирования из командной строки:

1. Преобразуйте свой пароль для удаления в шестнадцатеричный код.

   Воспользуйтесь интернет-ресурсом, средой программирования, текстовым редактором или другим инструментом для преобразования пароля в шестнадцатеричный код.

   Убедитесь, что разделитель вывода, используемый для разделения сгенерированного шестнадцатеричного кода на части, установлен на `00`. Например, шестнадцатеричный код `51 77 65 72 74 79` – неправильно, а шестнадцатеричный код `5100770065007200740079` – правильно.

2. Введите в командной строке следующую команду и нажмите на клавишу **ENTER**:

   `msiexec.exe /x{<product code>} /qn KLUNINSTPASSWD=<шестнадцатеричный код вашего пароля для удаления>`

   Вы можете найти код приложения вашего Агента администрирования в таблице ниже.

Коды приложения Агента администрирования

Язык локализации	Код приложения
Арабский	{FA7BF140-F356-404A-BDA3-3EF0878D7C63}
Болгарский	{4DBF6741-FA51-4C14-AFD2-B7D9246995F6}
Чешский	{478A6A0B-D177-4402-B703-808C05C56B13}
Английский	{BCF4CF24-88AB-45E1-A6E6-40C8278A70C5}
Французский	{2924BEDA-E0D7-4DAF-A224-50D2E0B12F5B}
Немецкий	{2F383CB3-6D7C-449D-9874-164E49E1E0F5}
Венгерский	{8899A4D4-D678-49F8-AD96-0B784F58D355}
Итальянский	{DC3A3164-36B3-4FB4-B7BF-16A41C35A728}
Японский	{790C176F-7780-4C84-8B9C-455F5C0E61C5}
Корейский	{70812A40-973B-4DA1-96B9-C2011280CD99}
Польский	{1A7B331A-ABBE-4230-995E-BCD99C5A18CF}
Португальский	{0F05E4E5-5A89-482C-9A62-47CC58643788}
Румынский	{FF802D76-E241-41D3-AAB4-DC7FBD659446}
Русский	{ED1C2D7E-5C7A-48D8-A697-57D1C080ABA7}

Упрощенный китайский	{FBD7C01E-49CB-4182-8714-9DB1EAE255CB}
Испанский	{F03982CF-1C5C-4E12-9F9E-D36C35E62402}
Испанский (Мексиканский)	{29748B5F-D88A-4933-B614-1CCCD6EFB0B7}
Традиционный китайский	{F6AD731A-36B4-4739-B1D4-70D6EDA35147}
Турецкий	{2475A66D-698B-4050-93FF-9B48EE82E2BA}

Использование средств удаленной установки приложений Kaspersky Security Center для запуска на управляемых устройствах произвольных исполняемых файлов

С помощью мастера создания инсталляционного пакета можно выбрать произвольный исполняемый файл и задать для него параметры командной строки. При этом в инсталляционный пакет можно поместить как сам выбранный файл, так и всю папку, в которой этот файл содержится. Затем следует создать задачу удаленной установки и выбрать созданный инсталляционный пакет.

В ходе работы задачи на устройствах будет запущен указанный при создании исполняемый файл с заданными параметрами командной строки.

Если используются инсталляторы в формате Microsoft Windows Installer (MSI), Kaspersky Security Center использует штатные возможности по анализу результата установки.

Если есть лицензия на Системное администрирование, при создании инсталляционного пакета для одного из поддерживаемых приложений, распространенных в корпоративной среде, Kaspersky Security Center также использует правила установки и анализа результатов установки, имеющиеся в его обновляемой базе.

В иных случаях для исполняемых файлов задача по умолчанию дожидается завершения запущенного процесса и всех порожденных им дочерних процессов. По завершении запущенных процессов задача будет завершена успешно независимо от кода возврата исходного процесса. Чтобы изменить такое поведение задачи, перед созданием задачи следует изменить вручную файлы с расширением .kpd, сформированные Kaspersky Security Center в папке созданного инсталляционного пакета и в его подпапках.

Файлы с расширением kpd используют кодировку ASCII. Файлы с расширением kud используют кодировку Юникод.

Для того чтобы задача не ожидала завершения запущенного процесса, в секции [SetupProcessResult] нужно задать значение 0 для параметра Wait:

```
[SetupProcessResult]
Wait=0
```

Для того чтобы на платформе Windows задача ожидала только завершения исходного процесса, но не порожденных им дочерних процессов, нужно в секции [SetupProcessResult] задать значение 0 для параметра WaitJob, например:

```
[SetupProcessResult]
WaitJob=0
```

Для того чтобы задача завершалась успешно или с ошибкой в зависимости от кода возврата запущенного процесса, создайте исполняемый файл с расширением bat, который сохранит код ошибки в файл, например:

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

Затем измените файлы с расширением kud, сформированные Kaspersky Security Center в папке созданного инсталляционного пакета:

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=Installation completed successfully.
[SetupMainResult_ErrorCodes]
1=Installation script error
2=Custom error
```

В этом случае любой код, отличный от перечисленных, будет означать ошибку.

Для того чтобы в результатах задачи отображалась строка с комментарием об успешном завершении задачи или сообщения об ошибках, нужно задать краткие описания ошибок, соответствующих кодам возврата процесса, в секциях [SetupProcessResult_SuccessCodes] и [SetupProcessResult_ErrorCodes], например:

```
[SetupProcessResult_SuccessCodes]
0= Installation completed successfully
3010=A reboot is required to complete the installation
[SetupProcessResult_ErrorCodes]
1602=Installation cancelled by the user
1603=Fatal error during installation
```

Для того чтобы задействовать средства Kaspersky Security Center по управлению перезагрузкой устройства (если перезагрузка необходима для завершения операции), нужно дополнительно перечислить коды возврата процесса, означающие необходимость перезагрузки, в секции [SetupProcessResult_NeedReboot]:

```
[SetupProcessResult_NeedReboot]
3010=
```

Мониторинг развертывания

Для контроля развертывания Kaspersky Security Center, а также для контроля наличия на управляемых устройствах приложения безопасности и Агента администрирования, следует обращать внимание на цветовой индикатор в блоке **Развертывание**. Индикатор расположен в рабочей области узла Сервер администрирования в главном окне Консоли администрирования. Индикатор отображает текущее состояние развертывания. Рядом с индикатором отображается количество устройств с установленными Агентами администрирования и приложениями безопасности. При наличии активных задач установки отображается прогресс выполнения задач. При наличии ошибок установки, здесь отображается количество ошибок. Просмотреть детальную информацию об ошибке можно по ссылке.

Также можно воспользоваться диаграммой развертывания в рабочей области папки **Управляемые устройства** на вкладке **Группы**. Диаграмма отражает процесс развертывания: количество устройств без Агента администрирования, с Агентом администрирования, с Агентом администрирования и приложением безопасности.

Более детальное описание хода развертывания (или работы конкретной задачи установки) можно увидеть в окне результатов выполнения соответствующей задачи удаленной установки: В контекстном меню задачи выберите **Результаты**. В окне отображаются два списка: в верхнем списке содержится список состояний задачи на устройствах, а в нижнем – список событий задачи на устройстве, которое в данный момент выбрано в верхнем списке.

Информация об ошибках при развертывании записывается в журнал событий Kaspersky Event Log Сервера администрирования. Информация об ошибках также доступна в соответствующей выборке событий в папке **Отчеты и уведомления**, в подпапке **События**.

Настройка параметров инсталляторов

В разделе содержится информация о файлах инсталляторов Kaspersky Security Center и параметрах установки, а также рекомендации по установке Сервера администрирования и Агента администрирования в "тихом" режиме.

Общая информация

Инсталляторы компонентов Kaspersky Security Center 15.1 – Сервера администрирования, Агента администрирования, Консоли администрирования – построены на технологии Windows Installer. Ядром инсталлятора является MSI-пакет. Этот формат упаковки дистрибутива позволяет использовать все преимущества технологии Windows Installer: масштабируемость, возможность использовать систему патчевания, систему трансформации, возможность установки централизованно сторонними решениями, прозрачность регистрации в операционной системе.

Установка в тихом режиме (с файлом ответов)

В инсталляторах Сервера администрирования и Агента администрирования реализована возможность работы с файлом ответов (ss_install.xml), в котором записаны параметры для установки в тихом режиме без участия пользователя. Файл ss_install.xml расположен в той же папке, что и MSI-пакет, и используется автоматически при установке в тихом режиме. Вы можете включить режим автоматической установки с помощью ключа командной строки "/s".

Пример запуска:

```
setup.exe /s
```

Прежде чем запускать приложение установки в тихом режиме, прочтите Лицензионное соглашение. Если в состав дистрибутива Kaspersky Security Center не входит TXT файл с текстом Лицензионного соглашения, вы можете загрузить этот файл с сайта "Лаборатории Касперского".

Файл ss_install.xml представляет собой внутренний формат параметров инсталлятора Kaspersky Security Center. В составе дистрибутивов поставляется файл ss_install.xml с параметрами по умолчанию.

Не следует изменять файл ss_install.xml вручную. Этот файл изменяется средствами Kaspersky Security Center при изменении параметров инсталляционных пакетов в Консоли администрирования.

Чтобы изменить файл ответов для установки Сервера администрирования:

1. Откройте дистрибутив Kaspersky Security Center. Если вы используете полный пакет EXE-файла, распакуйте его.
2. Сформируйте папку Сервер, откройте командную строку и выполните следующую команду:

   ```
   setup.exe /r ss_install.xml
   ```

   Запустится приложение установки Kaspersky Security Center.
3. Следуйте инструкциям мастера, чтобы настроить установку Kaspersky Security Center.

   По завершении работы мастера файл ответов автоматически изменится в соответствии с новыми параметрами, указанными вами.

Установка Агента администрирования в тихом режиме (без файла ответов)

Агент администрирования можно установить при помощи одного только msi-пакета, задавая при этом значения свойств MSI стандартным образом. Такой сценарий позволяет устанавливать Агент администрирования, используя групповые политики.

Не переименовывайте инсталляционный пакет Kaspersky Network Agent.msi. Переименование пакета может привести к ошибкам установки при обновлении Агента администрирования.

Для того чтобы не возникал конфликт между параметрами, заданными с помощью свойств MSI, и параметрами, заданными в файле ответов, предусмотрена возможность отключения файла ответов путем задания свойства `DONT_USE_ANSWER_FILE=1`. MSI-файл расположен в дистрибутиве приложения Kaspersky Security Center в папке Packages\NetAgent\exec. Ниже приведен пример запуска инсталлятора Агента администрирования с помощью msi-пакета.

Установка Агента администрирования в неинтерактивном режиме требует принятия Лицензионного соглашения. Используйте параметр EULA=1, только если вы полностью прочитали, понимаете и принимаете условия Лицензионного соглашения.

Пример:
```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

Также параметры инсталляции msi-пакета можно задать, подготовив предварительно файл трансформации (файл с расширением mst). Команда будет выглядеть следующим образом:

Пример:
```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

В одной команде можно указать более одного файла трансформации.

Если вы хотите обновить Агент администрирования с помощью установщика Windows Installer, выполните следующую команду:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Частичная настройка параметров установки через setup.exe

Запуская установку приложений через setup.exe, можно передавать в MSI-пакет значения любых свойств MSI.

Команда будет выглядеть следующим образом:

Пример:
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

Параметры установки Сервера администрирования

В таблице ниже описаны свойства MSI, которые можно настраивать при установке Сервера администрирования. Все параметры являются необязательными, кроме EULA и PRIVACYPOLICY.

Параметры установки Сервера администрирования в тихом режиме

Свойство MSI	Описание	Доступные значения
EULA	Согласие с условиями Лицензионного соглашения (обязательный параметр).	• 1 – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения настоящего Лицензионного соглашения. • Другое значение или не задано – не согласны с условиями Лицензионного соглашения (установка не выполняется).
PRIVACYPOLICY	Согласие с условиями Политики конфиденциальности (обязательный параметр).	• 1 – Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности. Я подтверждаю, что полностью прочитал(а) и понимаю Политику конфиденциальности. • Другое значение или не задано – Я не принимаю условия Политики конфиденциальности (установка не выполняется).
INSTALLATIONMODETYPE	Тип установки Сервера администрирования.	• Стандартная. • Выборочная.
INSTALLDIR	Папка установки приложения.	Строковое значение.

Свойство MSI	Описание	Доступные значения
ADDLOCAL	Список компонентов для установки (через запятую).	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Минимальный достаточный для корректной установки Сервера администрирования список компонентов: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Размер сети.	• NRT_1_100 – от 1 до 100 устройств. • NRT_100_1000 – от 101 до 1000 устройств. • NRT_GREATER_1000 – более 1000 устройств.
SRV_ACCOUNT_TYPE	Способ задания пользователя для работы службы Сервера администрирования.	• SrvAccountDefault – учетная запись пользователя будет создана автоматически. • SrvAccountUser – учетная запись пользователя задана вручную.
SERVERACCOUNTNAME	Имя пользователя для службы.	Строковое значение.
SERVERACCOUNTPWD	Пароль пользователя для службы.	Строковое значение.
DBTYPE	Тип базы данных.	• MySQL – будет использоваться база данных MySQL или MariaDB. • MSSQL – будет использоваться база данных Microsoft SQL Server (SQL Express).
MYSQLSERVERNAME	Полное имя сервера MySQL или MariaDB.	Строковое значение.
MYSQLSERVERPORT	Номер порта для подключения к серверу MySQL или MariaDB.	Числовое значение.
MYSQLDBNAME	Имя базы данных сервера MySQL или MariaDB.	Строковое значение.
MYSQLACCOUNTNAME	Имя пользователя для подключения к базе сервера MySQL или MariaDB.	Строковое значение.
MYSQLACCOUNTPWD	Пароль пользователя для подключения к базе сервера MySQL или MariaDB.	Строковое значение.
MSSQLCONNECTIONTYPE	Тип использования базы данных MSSQL.	• InstallMSSEE – установить из пакета. • ChooseExisting – использовать установленный сервер.
MSSQLSERVERNAME	Полное имя экземпляра SQL Server.	Строковое значение.
MSSQLDBNAME	Имя базы данных SQL Server.	Строковое значение.
MSSQLAUTHTYPE	Способ аутентификации при подключении к SQL Server.	• Windows. • SQLServer.
MSSQLACCOUNTNAME	Имя пользователя для подключения к SQL Server в режиме SQLServer.	Строковое значение.
MSSQLACCOUNTPWD	Пароль пользователя для подключения к SQL Server в режиме SQLServer.	Строковое значение.

CREATE_SHARE_TYPE	Способ задания папки общего доступа.	• Create – создать новую папку общего доступа. В этом случае должны быть заданы следующие свойства:
		  • SHARELOCALPATH – путь к локальной папке.
		  • SHAREFOLDERNAME – сетевое имя папки.
		• Пусто – должно быть задано свойство EXISTSHAREFOLDERNAME.

EXISTSHAREFOLDERNAME	Полный путь к существующей папке общего доступа.	Строковое значение.
SERVERPORT	Номер порта для подключения к Серверу администрирования.	Числовое значение.
SERVERSSLPORT	Номер порта для установки SSL-соединения с Сервером администрирования.	Числовое значение.

Свойство MSI	Описание	Доступные значения
SERVERADDRESS	Адрес Сервера администрирования.	Строковое значение.
SERVERCERT2048BITS	Длина ключа для сертификата Сервера администрирования (в битах).	• 1 – длина ключа для сертификата Сервера администрирования составляет 2048 бит. • 0 – длина ключа для сертификата Сервера администрирования составляет 1024 бит. • Если параметр не задан, длина ключа для сертификата Сервера администрирования составляет 2048 бит.
MOBILESERVERADDRESS	Адрес Сервера администрирования для подключения мобильных устройств; игнорируется, если не выбран компонент MobileSupport.	Строковое значение.

Параметры установки Агента администрирования

В таблице ниже описаны свойства MSI, которые можно настраивать при установке Агента администрирования. Все параметры являются необязательными, кроме SERVERADDRESS.

Свойства MSI

Свойство MSI	Описание	Доступные значения
DONT_USE_ANSWER_FILE	Читать параметры установки из файла ответов.	• 1 • Нет значения
INSTALLDIR	Папка установки.	
SERVERADDRESS	Адрес Сервера администрирования (обязательный параметр).	
SERVERPORT	Номер порта подключения к Серверу администрирования.	
SERVERSSLPORT	Номер порта для SSL-соединения.	
USESSL	Использовать ли SSL-соединение.	• 1 • Нет значения
OPENUDPPORT	Открыть ли UDP-порт.	• 1 • Нет значения
UDPPORT	Номер UDP-порта.	
USEPROXY	Использовать ли прокси-сервер.	• 1 • Нет значения
PROXYADDRESS	Адрес прокси-сервера.	
PROXYPORT	Номер порта подключения к Серверу администрирования.	
PROXYLOGIN	Учетная запись для подключения к прокси-серверу.	
PROXYPASSWORD	Пароль учетной записи для подключения к прокси-серверу. Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.	
GATEWAYMODE	Режим использования шлюза соединения.	• 0 – не использовать шлюз соединений; • 1 – использовать данный Агент администрирования в качестве шлюза соединений; • 2 – подключаться к Серверу администрирования через шлюз соединений.

Свойство MSI	Описание	Доступные значения
GATEWAYADDRESS	Адрес шлюза соединений.	
CERTSELECTION	Способ получения сертификата.	• GetOnFirstConnection – получить сертификат от Сервера администрирования; • GetExistent – выбрать существующий сертификат. Если выбран этот вариант, должно быть задано свойство CERTFILE.
CERTFILE	Путь к файлу сертификата.	
VMVDI	Включить динамический режим для VDI	• 1 • Нет значения
LAUNCHPROGRAM	Запускать ли службу Агента администрирования после установки.	• 1 • Нет значения

Виртуальная инфраструктура

Kaspersky Security Center поддерживает работу с виртуальными машинами. Вы можете установить Агент администрирования и приложения безопасности на каждую виртуальную машину, а также вы можете защищать виртуальные машины на уровне гипервизора. В первом случае для защиты виртуальных машин можно использовать как обычное приложение безопасности, так и Kaspersky Security для виртуальных сред Легкий агент. Во втором случае вы можете использовать Kaspersky Security для виртуальных сред Защита без агента.

Kaspersky Security Center поддерживает откат виртуальных машин к предыдущему состоянию.

Рекомендации по снижению нагрузки на виртуальные машины

В случае инсталляции Агента администрирования на виртуальную машину следует рассмотреть возможность отключения той части функциональности Kaspersky Security Center, которая не очень полезна для виртуальных машин.

При установке Агента администрирования на виртуальную машину или на шаблон, из которого в дальнейшем будут получены виртуальные машины, рекомендуется выполнить следующие действия:

- если выполняется удаленная установка, в окне свойств инсталляционного пакета Агента администрирования (в разделе **Дополнительно**) выбрать параметр **Оптимизировать параметры для VDI**;
- если выполняется интерактивная установка с помощью мастера, в окне мастера выбрать параметр **Оптимизировать параметры Агента администрирования для виртуальной инфраструктуры**.

Выбор параметров изменит параметры Агента администрирования таким образом, чтобы по умолчанию (до применения политики) были выключены следующие функции:

- получение информации об установленном программном обеспечении;
- получение информации об аппаратном обеспечении;
- получение информации о наличии уязвимостей;
- получение информации о необходимых обновлениях.

Как правило, перечисленные функции не нужны на виртуальных машинах в силу того, что программное обеспечение и виртуальное аппаратное обеспечение на них единообразны.

Выключение функций обратимо. Если любая из выключенных функций все же нужна, ее можно включить при помощи политики Агента администрирования, или в локальных параметрах Агента администрирования. Локальные параметры Агента администрирования доступны из контекстного меню соответствующего устройства в Консоли администрирования.

Поддержка динамических виртуальных машин

Kaspersky Security Center поддерживает динамические виртуальные машины. Если в сети организации развернута виртуальная инфраструктура, то в некоторых случаях могут использоваться динамические (временные) виртуальные машины. Такие машины создаются с уникальными именами из заранее подготовленного администратором шаблона. Пользователь работает с созданной машиной некоторое время, а после выключения виртуальная машина удаляется из виртуальной инфраструктуры. Если в сети организации развернут Kaspersky Security Center, то виртуальная машина с установленным на ней Агентом администрирования добавляется в базу данных Сервера администрирования. После выключения виртуальной машины запись о ней должна быть также удалена и из базы данных Сервера администрирования.

Чтобы функциональность автоматического удаления записей о виртуальных машинах работала, при установке Агента администрирования на шаблон, из которого будут созданы динамические виртуальные машины, нужно выбрать параметр **Включить динамический режим для VDI**:

- в случае удаленной установки – в окне свойств инсталляционного пакета Агента администрирования (раздел **Дополнительно**);
- в случае интерактивной установки – в мастере установки Агента администрирования.

> Параметр **Включить динамический режим для VDI** не следует выбирать при установке Агента администрирования на физические устройства.

Если нужно, чтобы события с динамических виртуальных машин сохранялись на Сервере администрирования некоторое время после удаления машин, то следует в окне свойств Сервера администрирования в разделе **Хранилище событий** выбрать параметр **Хранить события после удаления устройств** и указать максимальное время хранения событий в днях.

> Не рекомендуется включать шифрование дисков на динамических виртуальных машинах.

Поддержка копирования виртуальных машин

Копирование виртуальной машины с установленным на нее Агентом администрирования или ее создание из шаблона с установленным Агентом администрирования эквивалентно развертыванию Агентов администрирования захватом и копированием образа жесткого диска. Поэтому в общем случае при копировании виртуальных машин нужно выполнять те же действия, что и при развертывании копированием образа диска.

Однако в описанных ниже двух случаях Агент администрирования обнаруживает факт копирования автоматически. Поэтому выполнять сложные действия, описанные в разделе "Развертывание захватом и копированием жесткого диска устройства", необязательно:

- При установке Агента администрирования был выбран параметр **Включить динамический режим для VDI**: после каждой перезагрузки операционной системы такая виртуальная машина будет считаться новым устройством, независимо от факта ее копирования.

- Используется один из следующих гипервизоров: VMware™, HyperV® или Xen®: Агент администрирования определит факт копирования виртуальной машины по изменившимся идентификаторам виртуального аппаратного обеспечения.

Анализ изменений виртуального аппаратного обеспечения не абсолютно надежен. Прежде чем широко использовать данный метод, следует предварительно проверить его работоспособность на небольшом количестве виртуальных машин для используемой в организации версии гипервизора.

Поддержка отката файловой системы для устройств с Агентом администрирования

Kaspersky Security Center является распределенным приложением. Откат файловой системы в предыдущее состояние на одном из устройств с установленным Агентом администрирования приведет к рассинхронизации данных и неправильной работе Kaspersky Security Center.

Откат файловой системы (или ее части) в предыдущее состояние может происходить в следующих случаях:

- при копировании образа жесткого диска;

- при восстановлении состояния виртуальной машины средствами виртуальной инфраструктуры;

- при восстановлении данных из резервной копии или точки восстановления.

Для Kaspersky Security Center критичны только те сценарии, при которых стороннее программное обеспечение на устройствах с установленным Агентом администрирования затрагивает папку %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\. Поэтому следует всегда исключать эту папку из процедуры восстановления, если это возможно.

Поскольку в ряде организаций регламент работы предполагает выполнение отката состояния файловой системы устройств, в Kaspersky Security Center, начиная с версии 10 Maintenance Release 1 (Сервер администрирования и Агенты администрирования должны быть версии 10 Maintenance Release 1 или выше), была добавлена поддержка обнаружения отката файловой системы на устройствах с установленным Агентом администрирования. В случае обнаружения такие устройства автоматически переподключаются к Серверу администрирования с полной очисткой и полной синхронизацией данных.

В Kaspersky Security Center 15.1 поддержка обнаружения отката файловой системы включена по умолчанию.

Следует при любой возможности избегать отката папки %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ на устройствах с установленным Агентом администрирования, так как полная повторная синхронизация данных требует большого количества ресурсов.

Для устройства с установленным Сервером администрирования откат состояния системы недопустим. Недопустимым также является откат в предыдущее состояние базы данных, используемой Сервером администрирования.

Восстановить состояние Сервера администрирования из резервной копии можно только при помощи штатной утилиты klbackup.

О профилях соединения для автономных пользователей

При работе автономных пользователей, использующих ноутбуки (далее также "устройства"), может понадобиться изменить способ подключения к Серверу администрирования или переключиться между Серверами администрирования в зависимости от текущего положения устройства в сети.

Профили подключения поддерживаются только для устройств под управлением Windows и macOS.

Использование различных адресов одного и того же Сервера администрирования

Устройства с установленным Агентом администрирования могут в разные периоды времени подключаться к Серверу администрирования как из внутренней сети организации, так и из интернета. В этой ситуации может потребоваться, чтобы Агент администрирования использовал различные адреса для подключения к Серверу администрирования: внешний адрес Сервера при подключении из интернета и внутренний адрес Сервера при подключении из внутренней сети.

Для этого в свойствах политики Агента администрирования нужно добавить профиль для подключения к Серверу администрирования из интернета. Добавьте профиль в свойствах политики (раздел **Подключения**, вложенный раздел **Профили соединений**). В окне создания профиля необходимо выключить параметр **Использовать только для получения обновлений** и выбрать параметр **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**. Если для доступа к Серверу администрирования используется шлюз соединений (например, в конфигурации Kaspersky Security Center, описанной в разделе Доступ из интернета: Агент администрирования в качестве шлюза соединения в демилитаризованной зоне), в профиле подключения следует указать адрес шлюза соединения в соответствующем поле.

Переключение между Серверами администрирования в зависимости от текущей сети

Если в организации несколько офисов с различными Серверами администрирования и между ними перемещается часть устройств с установленным Агентом администрирования, то необходимо, чтобы Агент администрирования подключался к Серверу администрирования локальной сети того офиса, в котором находится устройство.

В этом случае в свойствах политики Агента администрирования следует создать профиль подключения к Серверу администрирования для каждого из офисов, за исключением домашнего офиса, в котором расположен исходный домашний Сервер администрирования. В профилях подключения следует указать адреса соответствующих Серверов администрирования и выбрать либо выключить параметр **Использовать только для получения обновлений**:

- выбрать параметр, если требуется, чтобы Агент администрирования синхронизировался с домашним Сервером администрирования, а локальный Сервер использовался только для загрузки обновлений;
- выключить параметр, если необходимо, чтобы Агент администрирования полностью управлялся локальным Сервером администрирования.

Далее необходимо настроить условия переключения на созданные профили: не менее одного условия для каждого из офисов, исключая "домашний офис". Смысл каждого такого условия заключается в обнаружении в сетевом окружении деталей, присущих одному из офисов. Если условие становится истинным, происходит активация соответствующего профиля. Если ни одно из условий не является истинным, Агент администрирования переключается на домашний Сервер администрирования.

Развертывание поддержки Управления мобильными устройствами

В этом разделе приведена информация о первоначальном развертывании функции Управление мобильными устройствами.

Подключение KES-устройств к Серверу администрирования

В зависимости от способа подключения устройств к Серверу администрирования существует две схемы развертывания Kaspersky Device Management для iOS для KES-устройств:

- схема развертывания с использованием прямого подключения устройств к Серверу администрирования;
- схема развертывания с использованием обратного прокси-сервера, поддерживающего Kerberos Constrained Delegation.

Прямое подключение устройств к Серверу администрирования

KES-устройства могут напрямую подключаться к порту 13292 Сервера администрирования.

В зависимости от способа аутентификации существуют два варианта подключения KES-устройств к Серверу администрирования:

- подключение устройств с использованием пользовательского сертификата;
- подключение устройств без пользовательского сертификата.

Подключение устройства с использованием пользовательского сертификата

При подключении устройства с использованием пользовательского сертификата происходит привязка этого устройства к учетной записи пользователя, для которой средствами Сервера администрирования назначен соответствующий сертификат.

В этом случае будет использована двусторонняя аутентификация SSL (mutual authentication). Как Сервер администрирования, так и устройство будут аутентифицированы с помощью сертификатов.

Подключение устройства без пользовательского сертификата

При подключении устройства без пользовательского сертификата оно не будет привязано ни к одной учетной записи пользователя на Сервере администрирования. Но при получении устройством любого сертификата будет произведена привязка этого устройства к пользователю, которому средствами Сервера администрирования назначен соответствующий сертификат.

При подключении устройства к Серверу администрирования будет использована односторонняя SSL-аутентификация (one-way SSL authentication), при которой только Сервер администрирования аутентифицируется с помощью сертификата. После получения устройством пользовательского сертификата тип аутентификации будет изменен на двустороннюю аутентификацию SSL (2-way SSL authentication, mutual authentication).

Схема подключения KES-устройств к Серверу с использованием принудительного делегирования Kerberos (KCD)

Схема подключения KES-устройств к Серверу администрирования с использованием Kerberos Constrained Delegation (KCD) предполагает:

- интеграция с обратным прокси-сервером, поддерживающим KCD;
- использование принудительного делегирования Kerberos Constrained Delegation (далее KCD) для аутентификации мобильных устройств;
- интеграцию с инфраструктурой открытых ключей (Public Key Infrastructure, далее PKI) для использования пользовательских сертификатов.

При использовании этой схемы подключения следует учесть следующее:

- Тип подключения KES-устройств к обратному прокси-серверу должен быть "two-way SSL authentication", то есть устройство должно подключаться к обратному прокси-серверу по своему пользовательскому сертификату. Для этого в инсталляционный пакет Kaspersky Endpoint Security для Android, который установлен на устройстве, необходимо интегрировать пользовательский сертификат. Этот KES-пакет должен быть создан Сервером администрирования специально для данного устройства (пользователя).
- Вместо серверного сертификата по умолчанию для мобильного протокола следует указать особый (кастомизированный) сертификат:

  1. В окне свойств Сервера администрирования в разделе **Параметры** установить флажок **Открыть порт для мобильных устройств** и в раскрывающемся списке выбрать **Добавить сертификат**.
  2. В открывшемся окне указать тот же сертификат, что задан на обратном прокси-сервере при публикации точки доступа к мобильному протоколу на Сервере администрирования.

- Пользовательские сертификаты для KES-устройств должны выписываться доменным Certificate Authority (CA). Следует учесть, если в домене несколько корневых CA, то пользовательские сертификаты должны быть выписаны тем CA, который прописан в публикации на обратном прокси-сервере.

  Обеспечить соответствие пользовательского сертификата заявленному выше требованию возможно несколькими способами:

  - Указать особый пользовательский сертификат в мастере создания инсталляционных пакетов и в мастере установки сертификатов.

  - Интегрировать Сервер администрирования с доменным PKI и настроить соответствующий параметр в правилах выписки сертификатов:

    1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Сертификаты**.

    2. В рабочей области папки **Сертификаты** по кнопке **Настроить правила выпуска сертификатов** откройте окно **Правила выпуска сертификатов**.

    3. В разделе **Интеграция с PKI** настройте интеграцию с инфраструктурой открытых ключей.

    4. В разделе **Выпуск мобильных сертификатов** укажите источник сертификатов.

Рассмотрим пример настройки ограниченного делегирования KCD со следующими допущениями:

- точка доступа к мобильному протоколу на Сервере администрирования поднята на 13292 порте;
- имя устройства с обратного прокси-сервера – firewall.mydom.local;
- имя устройства с Сервером администрирования – ksc.mydom.local;
- имя внешней публикации точки доступа к мобильному протоколу – kes4mob.mydom.global.

Доменная учетная запись для Сервера администрирования

Необходимо создать доменную учетную запись (например, KSCMobileSrvcUsr), под которой будет работать служба Сервера администрирования. Указать учетную запись для службы Сервера администрирования можно при установке Сервера администрирования или с помощью утилиты klsrvswch. Утилита klsrvswch расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Указать доменную учетную запись необходимо по следующим причинам:

- Функциональность по управлению KES-устройствами является неотъемлемой частью Сервера администрирования.
- Для правильной работы принудительного делегирования (KCD) принимающая сторона, которой является Сервер администрирования, должна работать под доменной учетной записью.

Service Principal Name для http/kes4mob.mydom.local

В домене под учетной записью KSCMobileSrvcUsr требуется прописать Service Principal Name (SPN) для публикации сервиса мобильного протокола на 13292 порту устройства с Сервером администрирования. Для устройства kes4mob.mydom.local с Сервером администрирования это будет выглядеть следующим образом:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

Настройка доменных свойств устройств с обратным прокси-сервером (firewall.mydom.local)

Для делегирования трафика нужно доверить устройство с обратным прокси-сервером (firewall.mydom.local) службе, определенной по SPN (http/kes4mob.mydom.local:13292).

Чтобы доверить устройство с обратным прокси-сервером службе, определенной по SPN (http/kes4mob.mydom.local:13292), администратору нужно выполнить следующие действия:

1. В оснастке Microsoft Management Console "Active Directory Users and Computers" выбрать устройство с установленным обратным прокси-сервером (firewall.mydom.local).

2. В свойствах устройства на вкладке **Delegation** для переключателя **Trust this computer for delegation to specified service only** выбрать вариант **Use any authentication protocol**.

3. В список **Services to which this account can present delegated credentials** добавить SPN http/kes4mob.mydom.local:13292.

Особый (кастомизированный) сертификат для публикации (kes4mob.mydom.global)

Для публикации мобильного протокола Сервера администрирования требуется выписать особый (кастомизированный) сертификат на FQDN kes4mob.mydom.global и указать его взамен серверного сертификата по умолчанию в параметрах мобильного протокола Сервера администрирования в Консоли администрирования. Для этого в окне свойств Сервера администрирования в разделе **Параметры** необходимо установить флажок **Открыть порт для мобильных устройств** и в раскрывающемся списке выбрать **Добавить сертификат**.

Следует учесть, что в контейнере с серверным сертификатом (файл с расширением p12 или pfx) должна также присутствовать цепочка корневых сертификатов (публичные части).

Настройка публикации на обратном прокси-сервере

На обратном прокси-сервере для трафика, идущего со стороны мобильного устройства на 13292 порт kes4mob.mydom.global, необходимо настроить KCD на SPN (http/kes4mob.mydom.local:13292) с использованием серверного сертификата, выписанного для FQND kes4mob.mydom.global. При этом следует учесть, что как на публикации, так и на публикуемой точке доступа (13292 порт Сервера администрирования) должен быть один и тот же серверный сертификат.

Использование Firebase Cloud Messaging

Для своевременной доставки команд на KES-устройства под управлением операционной системы Android в Kaspersky Security Center используется механизм push-нотификаций. Push-нотификации между KES-устройствами и Сервером администрирования осуществляются с помощью сервиса Firebase Cloud Messaging (далее – FCM). В Консоли администрирования Kaspersky Security Center вы можете указать параметры сервиса Cloud Messaging, чтобы подключить KES-устройства к этому сервису.

Для получения параметров Firebase Cloud Messaging вам необходимо иметь учетную запись Google.

Чтобы включить использование FCM:

1. В Консоли администрирования выберите узел **Управление мобильными устройствами** и папку **Мобильные устройства**.

2. В контекстном меню папки **Мобильные устройства** выберите пункт **Свойства**.

3. В окне свойств папки выберите раздел **Параметры Firebase Cloud Messaging**.

4. В поле **Номер проекта Firebase** укажите Sender ID FCM.

5. В поле **Файл приватного ключа (в формате JSON)** выберите файл приватного ключа.

   При следующей синхронизации с Сервером администрирования KES-устройства под управлением операционной системы Android будут подключены к службе Firebase Cloud Messaging.

Вы можете изменить параметры Firebase Cloud Messaging по кнопке **Сбросить параметры**.

При переключении на другой проект Firebase работа FCM возобновляется через 10 минут.

Сервис FCM работает на следующих диапазонах адресов:

- Со стороны KES-устройства необходим доступ на порты 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS), 5230 (HTTPS) следующих адресов:
  - google.com;
  - fcm.googleapis.com;
  - android.apis.google.com;
  - либо на все IP из списка "Google ASN 15169".
- Со стороны Сервера администрирования необходим доступ на порт 443 (HTTPS) следующих адресов:
  - fcm.googleapis.com;
  - либо на все IP из списка "Google ASN 15169".

В случае если в Консоли администрирования в свойствах Сервера администрирования заданы параметры прокси-сервера (**Дополнительно** / **Параметры доступа к сети Интернет**), то они будут использованы для взаимодействия с FCM.

При изменении значения `strDeviceRegId` устройства в таблице gcm_devices в серверной части FCM синхронизация измененного значения с серверной частью Kaspersky Security Center занимает 5 минут. Во время синхронизации сообщения могут поступать с задержкой на устройство, для которого было изменено значение `strDeviceRegId`.

Настройка FCM: получение Sender ID и файла закрытого ключа

Чтобы настроить FCM:

1. Зарегистрируйтесь на портале Google.

2. Перейдите в консоль Firebase.

3. Выполните одно из следующих действий:

   - Чтобы создать проект, нажмите на кнопку **Create a project** и следуйте инструкциям на экране.
   - Откройте существующий проект.

4. Нажмите на значок шестеренки и выберите **Project settings**.

   Откроется окно **Параметры проекта**.

5. Выберите вкладку **Cloud Messaging**.

6. Скопируйте Sender ID из поля **Sender ID** в разделе **Firebase Cloud Messaging API (V1)**.

7. Выберите вкладку **Service accounts** и нажмите на кнопку **Generate new private key**.

8. В открывшемся окне нажмите на кнопку **Generate key**, чтобы сгенерировать и загрузить файл приватного ключа.

Firebase Cloud Messaging настроен.

Интеграция с инфраструктурой открытых ключей

Интеграция с инфраструктурой открытых ключей (Public Key Infrastructure, далее PKI) в первую очередь предназначена для упрощения выпуска доменных пользовательских сертификатов Сервером администрирования.

Администратор может назначить для пользователя доменный сертификат в Консоли администрирования. Это можно сделать одним из следующих способов:

- назначить пользователю особый (кастомизированный) сертификат из файла в мастере установки сертификатов;
- выполнить интеграцию с PKI и назначить PKI источником сертификатов для конкретного типа сертификатов либо для всех типов сертификатов.

Параметры интеграции с PKI доступны в рабочей области папки **Управление мобильными устройствами** / **Сертификаты** при переходе по ссылке **Интегрировать с инфраструктурой открытых ключей**.

Общий принцип интеграции с PKI для выпуска доменных сертификатов пользователей

В Консоли администрирования по ссылке **Интегрировать с инфраструктурой открытых ключей** в рабочей области папки **Управление мобильными устройствами** / **Сертификаты** следует задать доменную учетную запись, которая будет использована Сервером администрирования для выписки доменных пользовательских сертификатов посредством доменного CA (далее – учетная запись, под которой производится интеграция с PKI).

Обратите внимание:

- В параметрах интеграции с PKI существует возможность указать шаблон по умолчанию для всех типов сертификатов. Тогда как в правилах выпуска сертификатов (правила доступны в рабочей области папки **Управление мобильными устройствами** / **Сертификаты** по кнопке **Настроить правила выпуска сертификатов**) присутствует возможность задать шаблон для каждого типа сертификата отдельно.

- На устройстве с установленным Сервером администрирования в хранилище сертификатов учетной записи, под которой производится интеграция с PKI, должен быть установлен специализированный сертификат Enrollment Agent (EA). Сертификат Enrollment Agent (EA) выписывает администратор доменного CA (Certificate Authority).

Учетная запись, под которой производится интеграция с PKI, должна соответствовать следующим критериям:

- Является доменным пользователем.

- Является локальным администратором устройства с установленным Сервером администрирования, с которого производится интеграция с PKI.

- Обладает правом *Вход в качестве службы*.

- Под этой учетной записью необходимо хотя бы один раз запустить устройство с установленным Сервером администрирования, чтобы создать постоянный профиль пользователя.

Веб-сервер Kaspersky Security Center

Веб-сервер Kaspersky Security Center (далее Веб-сервер) – это компонент Kaspersky Security Center. Веб-сервер предназначен для публикации автономных инсталляционных пакетов, автономных инсталляционных пакетов для мобильных устройств, а также файлов из папки общего доступа.

Созданные инсталляционные пакеты публикуются на Веб-сервере автоматически и удаляются после первой загрузки. Администратор может передать сформированную ссылку пользователю любым удобным способом, например, по электронной почте.

По полученной ссылке пользователь может загрузить на мобильное устройство предназначенную для него информацию.

Настройка Веб-сервера

Для тонкой настройки Веб-сервера в свойствах Веб-сервера можно сменить порты для протоколов HTTP (8060) и HTTPS (8061). Также, помимо смены портов, возможна смена серверного сертификата для HTTPS-протокола и смена FQDN-имени веб-сервера для HTTP-протокола.

Другие повседневные задачи

Этот раздел содержит рекомендации о ежедневной работе с Kaspersky Security Center.

Мониторинг цветовых индикаторов и зарегистрированных событий в Консоли администрирования

В Консоли администрирования можно быстро оценить текущее состояние Kaspersky Security Center и управляемых устройств с помощью цветовых индикаторов. Индикаторы отображаются в рабочей области узла **Сервер администрирования** на вкладке **Мониторинг**. На вкладке есть шесть информационных блоков с цветовыми индикаторами и зарегистрированными событиями. Цветной индикатор – это цветная вертикальная полоса на левой стороне панели. Каждый блок с индикатором отвечает за отдельную функциональную область Kaspersky Security Center (см. таблицу ниже).

Области ответственности цветовых индикаторов в Консоли администрирования

Название панели	Область ответственности цветового индикатора
Развертывание	Установка Агента администрирования и приложений безопасности на устройства сети организации.
Структура управления	Структура групп администрирования. Сканирование сети. Правила перемещения устройств.
Настройка защиты	Функции приложения безопасности: состояние защиты, поиск вредоносного ПО.
Обновление	Обновления и патчи.
Мониторинг	Состояние защиты.
Сервер администрирования	Функции и свойства Сервера администрирования.

Индикатор может быть одного из пяти цветов (см. таблицу ниже). Цвет индикатора зависит от текущего состояния Kaspersky Security Center и от зарегистрированных событий.

Цветовые кодировки индикаторов

Состояние	Цвет индикатора	Значение цвета индикатора
Информационное	Зеленый	Вмешательство администратора не требуется.
Предупреждение	Желтый	Требуется вмешательство администратора.
Предельный	Красный	Имеются серьезные проблемы. Требуется вмешательство администратора для их решения.
Информационное	Голубой	Зарегистрированы события, не связанные с угрозами для безопасности управляемых устройств.
Информационное	Серый	Информация о событиях недоступна или еще не получена.

Цель администратора – поддерживать индикаторы в состоянии "зеленый" на всех информационных панелях вкладки **Мониторинг**.

На информационных панелях также отображаются зарегистрированные события, влияющие на цветовые индикаторы, и состояние Kaspersky Security Center (см. таблицу ниже).

Название, описание и цвет индикатора зарегистрированных событий

Цвет индикатора	Отображаемое имя типа события	Тип события	Описание
Красный	**Количество устройств, на которых срок действия лицензии истек: %1**	IDS_AK_STATUS_LIC_EXPAIRED	События этого типа возникают, если срок действия коммерческой лицензии окончен. Один раз в день Kaspersky Security Center проверяет, не истек ли срок действия лицензии. После окончания срока действия коммерческой лицензии, Kaspersky Security Center работает в режиме Базовой функциональности. Чтобы продолжить использование Kaspersky Security Center, продлите срок действия коммерческой лицензии.

Цвет индикатора	Отображаемое имя типа события	Тип события	Описание
Красный	**Устройств с не запущенным приложением безопасности: %1**	IDS_AK_STATUS_AV_NOT_RUNNING	События этого типа возникают, когда приложение безопасности, установленное на устройстве, не запущено. Убедитесь, что на устройстве запущено приложение Kaspersky Endpoint Security.
Красный	**Устройств с выключенной защитой: %1**	IDS_AK_STATUS_RTP_NOT_RUNNING	События такого типа возникают, когда приложение защиты на устройстве отключено больше указанного времени. Проверьте текущий статус постоянной защиты на устройстве и убедитесь, что все необходимые вам компоненты защиты включены.
Красный	**Обнаружена уязвимость в программном обеспечении на устройствах**	IDS_AK_STATUS_VULNERABILITIES_FOUND	События этого типа происходят, когда задача *Поиск уязвимостей и требуемых обновлений* обнаружила уязвимости с указанным уровнем критичности в приложениях, установленных на устройстве. Проверьте список доступных обновлений в подпапке **Обновления программного обеспечения**, вложенной в папку **Управление приложениями**. Эта папка содержит список полученных Сервером администрирования обновлений приложений Microsoft и других производителей программного обеспечения, которые могут быть распространены на устройства. Просмотрите информацию о доступных обновлениях и установите их на устройство.
Красный	**На Сервере администрирования зарегистрированы критические события**	IDS_AK_STATUS_EVENTS_OCCURED	События этого типа возникают при обнаружении критических событий Сервера администрирования. Проверьте список событий, хранящихся на Сервере администрирования, а затем последовательно исправьте критические события.
Красный	**На Сервере администрирования зарегистрированы ошибки в событиях**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	События этого типа возникают при регистрации непредвиденных ошибок на стороне Сервера администрирования. Проверьте список событий, хранящихся на Сервере администрирования, а затем последовательно исправьте критические события.
Красный	**Потеряно соединение с устройствами: %1**	IDS_AK_STATUS_ADM_LOST_CONTROL1	События этого типа возникают при потере соединения между Сервером администрирования и устройством. Просмотрите список отключенных устройств и попробуйте подключить их снова.
Красный	**Устройств, которые давно не соединялись с Сервером администрирования: %1**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	События этого типа возникают, когда устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено. Убедитесь, что устройство включено и запущен Агент администрирования.
Красный	**Устройств со статусом отличным от "OK": %1**	IDS_AK_STATUS_HOST_NOT_OK	События этого типа происходят, когда статус устройства *OK*, подключенного к Серверу администрирования, меняется на *Критический* или *Предупреждение*. Устранить неполадку можно с помощью утилиты удаленной диагностики Kaspersky Security Center.

Цвет индикатора	Отображаемое имя типа события	Тип события	Описание
Красный	**Базы устарели: %1 устройств**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	События этого типа возникают, когда антивирусные базы на устройстве не обновлялись в течение заданного интервала времени. Следуйте инструкциям, чтобы обновить антивирусные базы "Лаборатории Касперского".
Красный	**Устройств, на которых давно не осуществлялась проверка обновлений Центра обновления Windows: %1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	События этого типа возникают, когда задача *Синхронизация обновлений Windows Update* не выполнялась больше указанного времени. Следуйте инструкциям, чтобы синхронизировать обновления из Центра обновления Windows Update с Сервером администрирования.
Красный	**Для Kaspersky Security Center требуется установка плагинов: %1**	IDS_AK_STATUS_PLUGINS_REQUIRED2	События этого типа возникают, когда вам нужно установить дополнительные плагины для приложений "Лаборатории Касперского". Загрузите и установите необходимые плагины управления для приложения "Лаборатории Касперского" с веб-сайта Службы технической поддержки "Лаборатории Касперского".

Удаленный доступ к управляемым устройствам

Этот раздел содержит информацию об удаленном доступе к управляемым устройствам.

Удаленное подключение к управляемым устройствам не поддерживается при доступе к Kaspersky Security Center Web Console с устройства с операционной системой Microsoft Windows на Arm.

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 не обеспечивает постоянного соединения между управляемыми устройствами и Сервером администрирования. Агенты администрирования на управляемых устройствах периодически устанавливают соединение и синхронизируются с Сервером администрирования. Продолжительность периода такой синхронизации задается в политике Агента администрирования. Если требуется предварительная синхронизация, Сервер администрирования (или точка распространения, если она используется) отправляет подписанный сетевой пакет по IPv4- или IPv6-сети на UDP-порт Агента администрирования. Номер порта по умолчанию – 15000. Если подключение по UDP от Сервера администрирования к управляемому устройству невозможно, то синхронизация произойдет при очередном периодическом подключении Агента администрирования к Серверу в течение периода синхронизации.

Некоторые операции невозможно выполнить без предварительного соединения Агента администрирования с Сервером администрирования, например, запуск и 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 соединения между управляемым устройством и Сервером администрирования.

Чтобы проверить постоянное соединение управляемого устройства с Сервером администрирования:

1. В дереве консоли выберите папку **Управляемые устройства**.
2. В рабочей области папки выберите управляемое устройство, с которым вы хотите обеспечить постоянную связь.
3. В контекстном меню устройства выберите пункт **Свойства**.

   Откроется окно свойств выбранного устройства.
4. В разделе **Общие** открывшегося окна 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.

О проверке времени соединения устройства с Сервером администрирования

При выключении устройства Агент администрирования уведомляет Сервер администрирования о выключении. В Консоли администрирования такое устройство отображается как выключенное. Однако Агенту удается уведомить Сервер администрирования не во всех случаях. Поэтому Сервер администрирования для каждого устройства периодически анализирует атрибут **Соединение с Сервером администрирования** (значение атрибута отображается в Консоли администрирования в свойствах устройства в разделе **Общие**) и сопоставляет его с периодом синхронизации из действующих параметров Агента администрирования. Если устройство не выходило на связь более чем три периода синхронизации, то такое устройство отмечается как выключенное.

О принудительной синхронизации

Несмотря на то что Kaspersky Security Center автоматически синхронизирует состояние, параметры, задачи и политики для управляемых устройств, в отдельных случаях администратору нужно точно знать, что в текущий момент для определенного устройства синхронизация выполнена.

В контекстном меню управляемых устройств в Консоли администрирования в пункте меню **Все задачи** имеется команда **Синхронизировать принудительно**. Когда Kaspersky Security Center 15.1 выполняет эту команду, Сервер администрирования пытается подключиться к устройству. Если эта попытка успешна, будет выполнена принудительная синхронизация. В противном случае принудительная синхронизация произойдет только после очередного выхода Агента администрирования на связь с Сервером.

О туннелировании

Kaspersky Security Center 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.

В частности, туннелирование используется для подключения к удаленному рабочему столу: как для подключения к существующему сеансу, так и для создания нового удаленного сеанса.

Также туннелирование может быть использовано при помощи механизма внешних инструментов. В частности, администратор может запускать таким образом утилиту putty, VNC-клиент и прочие инструменты.

Руководство по масштабированию

В этом руководстве представлена информация по масштабированию Kaspersky Security Center.

Об этом руководстве

Руководство по масштабированию Kaspersky Security Center 15.1 (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 (в том числе мобильных) с установленным программным обеспечением "Лаборатории Касперского". Если мобильные (или любые другие) управляемые устройства, необходимо рассматривать отдельно, это специально оговаривается.

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 ключевых узлов Kaspersky Security Center – Серверов администрирования и точек распространения:
  - об аппаратных требованиях к Серверам администрирования и к точкам распространения;
  - о расчете количества и иерархии Серверов администрирования;
  - о расчетах количества и конфигурации точек распространения.
- 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 установкой Kaspersky Security Center;
- при планировании существенных изменений размеров сети, в которой развернут Kaspersky Security Center;

- при переходе от использования Kaspersky Security Center в ограниченном сегменте сети (тестовая среда) к полномасштабному развертыванию Kaspersky Security Center в корпоративной сети;
- при изменениях в наборе используемых функций Kaspersky Security Center.

Информация об ограничениях Kaspersky Security Center

В таблице ниже приведены ограничения текущей версии Kaspersky Security Center.

Ограничения Kaspersky Security Center

Тип ограничения	Значение
Максимальное количество управляемых устройств на один Сервер администрирования	100 000
Максимальное количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**	300
Максимальное количество групп администрирования	10 000
Максимальное количество хранимых событий	45 000 000
Максимальное количество политик	2000
Максимальное количество задач	2000
Максимальное суммарное количество объектов Active Directory (подразделений и учетных записей пользователей, устройств и групп безопасности)	1 000 000
Максимальное количество профилей в политике	100
Максимальное количество подчиненных Серверов у одного главного Сервера администрирования	500
Максимальное количество виртуальных Серверов администрирования	500
Максимальное количество устройств, которые может обслуживать одна точка распространения (точки распространения могут обслуживать только немобильные устройства)	10 000
Максимальное количество устройств, которые могут использовать один шлюз соединения	10 000, включая мобильные устройства
Максимальное количество мобильных устройств на один Сервер администрирования	100 000 минус количество стационарных управляемых устройств

Расчеты для Серверов администрирования

В этом разделе приведены аппаратные и программные требования для устройств, которые используются в качестве Серверов администрирования. Также даны рекомендации для расчета количества Серверов администрирования и их иерархии, в зависимости от конфигурации сети организации.

Расчет аппаратных ресурсов для Сервера администрирования

В этом разделе приведены расчеты, которыми можно руководствоваться при планировании аппаратных ресурсов для Сервера администрирования. Отдельно приводится рекомендация по расчету места на диске при использовании Системного администрирования.

Аппаратные требования для СУБД и Сервера администрирования

В таблицах ниже приведены рекомендуемые минимальные аппаратные требования СУБД и Сервера администрирования, полученные в ходе тестирования. Полный список поддерживаемых операционных систем и СУБД см. в перечне аппаратных и программных требований.

Сервер администрирования и СУБД на разных устройствах, в сети 50 000 устройств

Конфигурация устройства с Сервером администрирования

Оборудование	Значение
Процессор	4 ядра, 2500 МГц
ОЗУ	8 ГБ
Жесткий диск	300 ГБ, желателен RAID
Сетевой адаптер	1 Гбит

Конфигурация устройства с СУБД

Оборудование	Значение
Процессор	4 ядра, 2500 МГц
ОЗУ	16 ГБ
Жесткий диск	200 ГБ SATA RAID
Сетевой адаптер	1 Гбит

Сервер администрирования и СУБД на одном устройстве, в сети 50 000 устройств

Конфигурация устройства с Сервером администрирования и СУБД

Оборудование	Значение
Процессор	8 ядер, 2500 МГц
ОЗУ	16 ГБ
Жесткий диск	500 ГБ SATA RAID
Сетевой адаптер	1 Гбит

Сервер администрирования и СУБД на разных устройствах, в сети 100 000 устройств

Конфигурация устройства с Сервером администрирования

Оборудование	Значение
Процессор	8 ядер, 2,13 ГГц
ОЗУ	8 ГБ

Оборудование	Значение
Жесткий диск	1 ТБ, RAID
Сетевой адаптер	1 Гбит

Конфигурация устройства с СУБД

Оборудование	Значение
Процессор	8 ядер, 2,53 ГГц
ОЗУ	26 ГБ
Жесткий диск	500 ГБ SATA RAID
Сетевой адаптер	1 Гбит

Тестирование проводилось со следующими настройками:

- на Сервере администрирования включено автоматическое назначение точек распространения, либо точки распространения назначены вручную по рекомендуемой таблице;
- задача резервного копирования сохраняет резервные копии на файловый ресурс, расположенный на отдельном сервере;
- период синхронизации Агентов администрирования настроен в соответствии с таблицей ниже.

Период синхронизации Агентов администрирования

Период синхронизации, минуты	Количество управляемых устройств
15	10 000
30	20 000
45	30 000
60	40 000
75	50 000
150	100 000

Расчет места в базе данных

Место, которое будет занято в базе данных, можно приблизительно оценить по следующей формуле:

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), КБ,

где:

- "C" – количество устройств.

  Если в состав управляемых устройств входят динамические виртуальные машины, C – это сумма количества нединамических управляемых устройств и количества динамических виртуальных машин с Агентом администрирования, созданных между двумя последовательными запусками задачи **Обслуживание Сервера администрирования**.

- "E" – количество сохраняемых событий.

- "A" – суммарное количество объектов Active Directory:
  - учетных записей устройств;
  - учетных записей пользователей;
  - учетных записей групп безопасности;
  - подразделений Active Directory.

  Если сканирование Active Directory выключено, то "A" следует считать равным нулю.
- N – среднее количество инвентаризируемых исполняемых файлов на конечном устройстве.
- F – количество конечных устройств, на которых были инвентаризированы исполняемые файлы.

Если вы планируете включить в параметрах политики Kaspersky Endpoint Security информирование Сервера администрирования о запускаемых приложениях, то для хранения информации о запускаемых приложениях в базе данных дополнительно потребуется (0,03 * C) ГБ.

Если Сервер администрирования распространяет обновления Windows (играет роль Windows Server Update Services), то в базе данных дополнительно потребуется 2,5 ГБ.

В ходе работы в базе данных всегда образуется так называемое *незанятое пространство* (unallocated space). Поэтому реальный размер файла базы данных (по умолчанию файл KAV.MDF в случае использования СУБД "SQL Server") часто оказывается примерно в два раза больше, чем занятое в базе данных место.

Не рекомендуется явно ограничивать размер журнала транзакций (по умолчанию файл KAV_log.LDF, если вы используете SQL Server в качестве СУБД). Рекомендуется оставить значение параметра MAXSIZE по умолчанию. Если вам необходимо ограничить размер этого файла, нужно учесть, что необходимое минимальное значение параметра MAXSIZE для KAV_log.LDF составляет 20 480 МБ.

Расчет места на диске (с учетом и без учета использования Системного администрирования)

Расчет места на диске без учета использования Системного администрирования

Место на диске Сервера администрирования, требуемое для папки %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit, можно приблизительно оценить по формуле:

(724 * C + 0.15 * E + 0.17 * A), КБ

где:

- "C" – количество устройств.

  Если в состав управляемых устройств входят динамические виртуальные машины, C – это сумма количества нединамических управляемых устройств и количества динамических виртуальных машин с Агентом администрирования, созданных между двумя последовательными запусками задачи **Обслуживание Сервера администрирования**.

- "E" – количество сохраняемых событий.
- "A" – суммарное количество объектов Active Directory:
  - учетных записей устройств;
  - учетных записей пользователей;
  - учетных записей групп безопасности;
  - подразделений Active Directory.

Если сканирование Active Directory выключено, то "A" следует считать равным нулю.

Расчет дополнительного места на диске с учетом использования Системного администрирования

- Обновления. В папке общего доступа требуется дополнительно не менее 4 ГБ для хранения обновлений.
- Инсталляционные пакеты. При наличии на Сервере администрирования инсталляционных пакетов в папке общего доступа дополнительно потребуется количество места, равное суммарному размеру устанавливаемых имеющихся инсталляционных пакетов.
- Задачи удаленной установки. При наличии на Сервере администрирования задач удаленной установки на диске дополнительно потребуется количество места на диске (в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit), равное суммарному размеру устанавливаемых инсталляционных пакетов.
- Патчи. Если Сервер администрирования используется для установки патчей, то потребуется дополнительное место на диске:
  - Папка для хранения патчей должна иметь объем дискового пространства, равный суммарному размеру всех загруженных патчей. По умолчанию патчи хранятся в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles.

    Вы можете использовать утилиту klsrvswch, чтобы указать другую папку для хранения патчей. Утилита klsrvswch расположена в папке установки Сервера администрирования. Путь установки по умолчанию: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

    Если Сервер администрирования используется в качестве WSUS, то рекомендуется зарезервировать под эту папку не менее 100 ГБ.
  - В папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit – количество места, равное суммарному размеру тех патчей, на которые ссылаются имеющиеся экземпляры задачи установки обновлений (патчей) и закрытия уязвимостей.

Расчет количества и конфигурации Серверов администрирования

Чтобы снизить нагрузку на главный Сервер администрирования, вы можете назначить в каждую группу администрирования отдельный Сервер администрирования. Количество Серверов администрирования, подчиненных главному Серверу, не может превышать 500.

Рекомендуется выстраивать конфигурацию Серверов администрирования в зависимости от того, как настроена сеть в вашей организации.

Рекомендации по подключению динамических виртуальных машин к Kaspersky Security Center

Динамические виртуальные машины потребляют больше ресурсов, чем статические виртуальные машины.

Дополнительные сведения о динамических виртуальных машинах см. Поддержка динамических виртуальных машин.

При подключении новой динамической виртуальной машины Kaspersky Security Center создает значок этой динамической виртуальной машины в Консоли администрирования и перемещает динамическую виртуальную машину в группу администрирования. После этого динамическая виртуальная машина добавляется в базу данных Сервера администрирования. Сервер администрирования полностью синхронизирован с Агентом администрирования, установленным на этой динамической виртуальной машине.

В сети организации Агент администрирования создает для каждой динамической виртуальной машины следующие сетевые списки:

- оборудование;
- установленное программное обеспечение;
- обнаруженные уязвимости;
- события и списки исполняемых файлов компонента Контроль приложений.

Агент администрирования передает эти сетевые списки на Сервер администрирования. Размер сетевых списков зависит от компонентов, установленных на динамической виртуальной машине, и может влиять на производительность Kaspersky Security Center и системы управления базами данных (СУБД). Обратите внимание, что нагрузка может расти нелинейно.

После того, как пользователь заканчивает работу с динамической виртуальной машиной и выключает ее, эта машина удаляется из виртуальной инфраструктуры, записи о ней удаляются из базы данных Сервера администрирования.

Все эти действия используют много ресурсов базы данных Kaspersky Security Center и Сервера администрирования и могут снизить производительность Kaspersky Security Center и СУБД. Рекомендуется подключать к Kaspersky Security Center до 20 000 динамических виртуальных машин.

Вы можете подключить к Kaspersky Security Center более 20 000 динамических виртуальных машин, если подключенные динамические виртуальные машины выполняют стандартные операции (например, обновление баз) и потребляют не более 80% памяти и 75–80% доступных ядер.

Изменение параметров политики, программного обеспечения или операционной системы на динамической виртуальной машине может уменьшить или увеличить потребление ресурсов. Оптимальным считается потребление 80–95% ресурсов.

Расчеты для точек распространения и шлюзов соединений

В этом разделе приведены аппаратные требования к устройствам, которые используются в качестве точек распространения, и рекомендации по расчету количества точек распространения и шлюзов соединений в зависимости от конфигурации сети организации.

Требования для точки распространения

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.

> Не рекомендуется назначать Сервер администрирования в качестве точки распространения, так как это увеличит нагрузку на Сервер администрирования.

При наличии на Сервере администрирования задач удаленной установки, на устройстве с точкой распространения дополнительно потребуется дисковое пространство, равное суммарному размеру устанавливаемых инсталляционных пакетов.

При наличии на Сервере администрирования одного или нескольких экземпляров задачи установки обновлений (патчей) и закрытия уязвимостей на устройстве с точкой распространения дополнительно потребуется дисковое пространство, равное удвоенному суммарному размеру всех устанавливаемых патчей.

Если вы используете схему, по которой точки распространения получают обновления баз и модулей приложений напрямую с серверов обновлений "Лаборатории Касперского", точки распространения должны быть подключены к сети интернет.

Расчет количества и конфигурации точек распространения

Чем больше клиентских устройств содержит сеть, тем больше требуется точек распространения. Рекомендуется не отключать автоматическое назначение точек распространения. При включенном автоматическом назначении точек распространения Сервер администрирования назначает точки распространения, если число клиентских устройств достаточно велико, и определяет их конфигурацию.

Использование специально выделенных точек распространения

Если вы планируете использовать в качестве точек распространения какие-то определенные устройства (например, выделенные для этого серверы), то можно не использовать автоматическое назначение точек распространения. В этом случае убедитесь, что устройства, которые вы хотите назначить точками распространения, имеют достаточно свободного места на диске, их не отключают регулярно и на них выключен "спящий режим".

Число специально выделенных точек распространения в сети, содержащей один сегмент сети, в зависимости от количества устройств в сети

Число клиентских устройств в сегменте сети	Количество точек распространения
Менее 300	0 (точки распространения не нужны)
Более 300	Приемлемо: (N/10 000 + 1), рекомендуется: (N/5000 + 2), где N количество устройств в сети

Число специально выделенных точек распространения в сети, содержащей несколько сегментов сети, в зависимости от количества устройств в сети

Число клиентских устройств в каждом сегменте сети	Количество точек распространения
Менее 10	0 (точки распространения не нужны)
10–100	1
Более 100	Приемлемо: (N/10 000 + 1), рекомендуется: (N/5000 + 2), где N количество устройств в сети

Использование клиентских устройств (рабочих станций) в качестве точек распространения

Если вы планируете использовать в качестве точек распространения обычное клиентское устройство (рабочую станцию), то рекомендуется назначать точку распространения, как показано в таблице ниже, чтобы избежать чрезмерной нагрузки на каналы связи и Сервер администрирования:

Число рабочих станций, выполняющих роль точек распространения в сети, которая содержит один сегмент сети, в зависимости от количества сетевых устройств

Число клиентских устройств в сегменте сети	Количество точек распространения
Менее 300	0 (точки распространения не нужны)
Более 300	(N/300 +1), где N – число устройств в сети; не менее 3 точек распространения

Число рабочих станций, выполняющих роль точек распространения в сети, которая содержит несколько сегментов сети, в зависимости от количества сетевых устройств

Число клиентских устройств в каждом сегменте сети	Количество точек распространения
Менее 10	0 (точки распространения не нужны)
10–30	1
31–300	2
Более 300	(N/300 +1), где N – число устройств в сети; не менее 3 точек распространения

Если точка распространения отключена или по другим причинам недоступна, то управляемые устройства из области действия этой точки распространения могут обращаться за обновлениями к Серверу администрирования.

Расчет количества шлюзов соединений

Если вы планируете использовать шлюз соединений, рекомендуется использовать выделенное устройство для этой функции.

Один шлюз соединений обслуживает не более 10 000 управляемых устройств, включая мобильные устройства.

Хранение информации о событиях для задач и политик

В этом разделе приведены расчеты, связанные с хранением событий в базе данных Сервера администрирования, и даны рекомендации, как минимизировать количество событий и таким образом снизить нагрузку на Сервер администрирования.

По умолчанию в свойствах каждой задачи и каждой политики указано сохранение в журнале всех событий, связанных с выполнением задачи и применением политики.

Однако если задача запускается достаточно часто (например, более одного раза в неделю) и на достаточно большом количестве устройств (например, более 10 000), количество событий может оказаться слишком большим, и события могут заполнить базу данных. В таком случае рекомендуется указать в свойствах задачи один из двух других вариантов:

- **Сохранять события, связанные с ходом выполнения задачи**. В этом случае с каждого устройства, на котором выполнена задача, в базу данных поступает только информация о запуске задачи, о ее ходе и о ее выполнении (успешном, с предупреждением либо с ошибкой).

- **Сохранять только результат выполнения задачи**. В этом случае с каждого устройства, на котором выполнена задача, в базу данных поступает только информация о выполнении задачи (успешном, с предупреждением либо с ошибкой).

Если политика определена для достаточно большого количества устройств (например, более 10 000), количество событий также может оказаться слишком большим, и события могут заполнить базу данных. В таком случае рекомендуется выбрать в свойствах политики только наиболее важные события и включить их сохранение. Сохранение всех других событий рекомендуется отключить.

Таким образом вы уменьшаете количество событий в базе данных, увеличиваете скорость работы сценариев, связанных с анализом таблицы событий в базе данных, и снижаете риск вытеснения критических событий большим количеством событий.

Вы также можете уменьшить срок хранения событий, связанных с задачей или политикой. По умолчанию этот срок составляет семь дней для событий, связанных с задачей, и 30 дней для событий, связанных с политикой. При изменении срока хранения событий принимайте в расчет порядок работы, принятый в вашей организации, и количество времени, которое системный администратор может уделять анализу каждого события.

Вносить изменения в параметры хранения событий целесообразно в любом из следующих случаев:

- события об изменении промежуточных состояний групповых задач и о применении политик занимают значительный процент всех событий в базе данных Kaspersky Security Center;
- в журнале событий Kaspersky Event Log появляются записи об автоматическом удалении событий при превышения заданного лимита на общее число событий, хранимых в базе данных.

Выберите параметры регистрации событий, исходя из того, что оптимальное количество событий, поступающих с одного устройства в день, не должно превышать 20. Вы можете немного увеличить максимальное количество событий, если это необходимо, но только в том случае, если количество устройств в вашей сети относительно невелико (менее 10 000).

Особенности и оптимальные параметры некоторых задач

Некоторые задачи имеют особенности, связанные с количеством устройств в сети. В этом разделе даны рекомендации по оптимальной настройке параметров для таких задач.

Обнаружение устройств, задача резервного копирования данных, задача обслуживания Сервера администрирования и групповые задачи обновления Kaspersky Endpoint Security входят в базовую функциональность Kaspersky Security Center.

Частота обнаружения устройств

Не рекомендуется увеличивать установленную по умолчанию частоту поиска устройств, так как это может создать чрезмерную нагрузку на контроллеры домена. Рекомендуется, наоборот, устанавливать расписание опроса с минимально возможной частотой, насколько позволяют потребности вашей организации. В таблице ниже приведены рекомендации по расчету оптимального расписания.

Расписание обнаружения устройств

Количество устройств в сети	Рекомендуемая частота для обнаружения устройств
Менее 10 000	Установленная по умолчанию или реже
10 000 и более	Один раз в сутки или реже

Задачи резервного копирования данных Сервера администрирования и обслуживания Сервера администрирования

Сервер администрирования перестает функционировать во время выполнения следующих задач:

- Резервное копирование данных Сервера администрирования
- Обслуживание Сервера администрирования

Пока выполняются эти задачи, данные не могут поступать в базу данных.

Вам может потребоваться изменить расписание этих задач так, чтобы их выполнение не пересекалось по времени с выполнением других задач Сервера администрирования.

Групповые задачи обновления Kaspersky Endpoint Security

Если источником обновлений является Сервер администрирования, то для групповых задач обновления Kaspersky Endpoint Security версии 10 и выше рекомендуется расписание **При загрузке обновлений в хранилище** с установленным флажком **Автоматически определять интервал для распределения запуска задачи**.

Если вы создали на каждой точке распространения локальную задачу загрузки обновлений в хранилище с серверов "Лаборатории Касперского", то для групповой задачи обновления Kaspersky Endpoint Security рекомендуется задать периодическое расписание. Значение периода автономизации в этом случае должно составлять один час.

Задача Инвентаризации

Вы можете снизить нагрузку на базу данных при получении информации об исполняемых файлах. Для этого рекомендуется запускать задачу инвентаризации для Kaspersky Endpoint Security на нескольких эталонных устройствах, на которых установлен стандартный набор приложений.

Количество исполняемых файлов, получаемых Сервером администрирования от одного устройства, не может превышать 150 000. При достижении этого ограничения Kaspersky Security Center не получит новые файлы.

Количество файлов на обыкновенном клиентском устройстве, как правило, составляет не более 60 000. Количество исполняемых файлов на файловом сервере может быть больше и может даже превышать порог в 150 000.

Тестовые замеры показали, что на устройстве под управлением операционной системы Windows 7, на котором установлено приложение Kaspersky Endpoint Security 11 и не установлены никакие сторонние приложения, результаты выполнения задачи инвентаризации следующие:

- Когда флажки **Инвентаризация DLL-модулей** и **Инвентаризации файлов скриптов** сняты: около 3000 файлов.
- Когда флажки **Инвентаризация DLL-модулей** и **Инвентаризации файлов скриптов** установлены: от 10 000 до 20 000 файлов, в зависимости от количества установленных пакетов обновлений операционной системы.
- Когда установлен только флажок **Инвентаризации файлов скриптов**: приблизительно 10 000 файлов.

Информация о нагрузке на сеть между Сервером администрирования и защищаемыми устройствами

В этом разделе приводятся результаты тестовых замеров трафика в сети с указанием условий, при которых проводились замеры. Вы можете использовать эту информацию как справочную при планировании сетевой инфраструктуры и пропускной способности каналов внутри организации (либо между Сервером администрирования и организацией, в которой расположены защищаемые устройства). Зная пропускную способность сети, вы также можете приблизительно оценивать, сколько времени должна занять та или иная операция, связанная с передачей данных.

Потребление трафика выполнении различных сценариев

В таблице ниже приводятся результаты тестовых замеров трафика между Сервером администрирования и управляемым устройством при выполнении различных сценариев.

Синхронизация устройства с Сервером администрирования происходит по умолчанию раз в 15 минут либо реже. Однако если вы меняете на Сервере администрирования параметры политики или задачи, то происходит досрочная синхронизация устройств, для которых применима эта политика (или задача), и новые параметры передаются на устройства.

Трафик между Сервером администрирования и управляемым устройством

Сценарий	Трафик от Сервера к каждому управляемому устройству	Трафик от каждого управляемого устройства к Серверу
Установка Kaspersky Endpoint Security 11.7 для Windows с обновленными базами	390 МБ	3.3 МБ
Установка Агента администрирования	75 МБ	397 КБ
Совместная установка Агента администрирования и Kaspersky Endpoint Security 11.7 для Windows	459 МБ	3.6 МБ
Первоначальное обновление антивирусных баз без обновления баз в пакете (если участие в Kaspersky Security Network выключено)	113 МБ	1,8 МБ
Ежесуточное обновление антивирусных баз (если участие в Kaspersky Security Network включено)	22 МБ	373 МБ
Первоначальная синхронизация до обновления баз на устройстве (передача политик и задач)	382 КБ	446 КБ
Первоначальная синхронизация после обновления баз на устройстве	20 КБ	157 КБ
Синхронизация при отсутствии изменений на Сервере администрирования (по расписанию)	18 КБ	23 КБ
Синхронизация при изменении одного параметра в политике группы (досрочная, сразу после внесения изменения)	19 КБ	20 КБ
Синхронизация при изменении одного параметра в групповой задаче (досрочная, сразу после внесения изменения)	14 КБ	11 КБ
Принудительная синхронизация	110 КБ	109 КБ
Событие **Обнаружен вирус** (1 вирус)	44 КБ	50 КБ
Событие **Обнаружен вирус** (10 вирусов)	58 КБ	77 КБ
Разовый трафик после включения списка реестра приложений	до 10 КБ	до 12 КБ
Ежедневный трафик при включенном списке реестра приложений	до 840 КБ	до 1 МБ

Средний расход трафика за сутки

Средний расход трафика за сутки между Сервером администрирования и управляемым устройством:

- Трафик от Сервера к управляемому устройству – 840 КБ.
- Трафик от управляемого устройства к Серверу – 1 МБ.

Трафик был измерен при следующих условиях:

- На управляемом устройстве были установлены Агент администрирования и Kaspersky Endpoint Security 11.6 для Windows.
- Устройство не было назначено точкой распространения.
- Системное администрирование не было включено.
- Период синхронизации с Сервером администрирования составляло 15 минут.

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, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Security Center.

Kaspersky предоставляет поддержку Kaspersky Security Center в течение жизненного цикла (см. страницу жизненного цикла приложений). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;

- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки.

Получение файлов дампа Сервера администрирования

Файлы дампа Сервера администрирования содержат всю информацию о процессах Сервера администрирования на определенный момент времени. Файлы дампа Сервера администрирования хранятся в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\~dumps. Файлы дампа хранятся, пока используется Kaspersky Security Center, и удаляются безвозвратно при удалении приложения. Файлы дампа не отправляются в "Лабораторию Касперского" автоматически.

В случае сбоя Сервера администрирования вы можете обратиться в Службу технической поддержки "Лаборатории Касперского". Специалист Службы технической поддержки может попросить вас отправить файлы дампа Сервера администрирования для дальнейшего анализа в "Лабораторию Касперского".

Файлы дампа могут содержать персональные данные. Перед отправкой в "Лабораторию Касперского" рекомендуется защитить информацию от несанкционированного доступа.

Источники информации о приложении

Страница Kaspersky Security Center на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Security Center вы можете получить общую информацию о приложении, его возможностях и особенностях работы.

Страница Kaspersky Security Center в Базе знаний

База знаний – это раздел на веб-сайте Службы технической поддержки "Лаборатории Касперского".

На странице Kaspersky Security Center в Базе знаний вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи в Базе знаний могут дать ответы на вопросы, связанные с Kaspersky Security Center и с другими приложениями "Лаборатории Касперского". Также в статьях Базы знаний могут быть новости Службы технической поддержки.

Обсуждение приложений "Лаборатории Касперского" в сообществе пользователей

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем Форуме.

На Форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

> Для отображения онлайн-справки требуется соединение с интернетом.

Если вы не нашли решения вашего вопроса, обратитесь в Службу технической поддержки.

Глоссарий

AWS Application Program Interface (AWS API)

Программный интерфейс приложения платформы AWS, который используется приложением Kaspersky Security Center. 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*.

FileTransferBridge

Внутренний компонент Kaspersky Security Center, который обеспечивает локальную доставку обновлений приложений "Лаборатории Касперского". FileTransferBridge интегрирован в Агент администрирования (klnagent) и запускается локально на каждом управляемом устройстве.

Когда приложения "Лаборатории Касперского" получают обновления от Kaspersky Security Center, Агент администрирования загружает файлы обновлений с Сервера администрирования или с точки распространения. Затем FileTransferBridge передает файлы локально установленным приложениям "Лаборатории Касперского", обеспечивая надежную доставку обновлений баз данных и патчей.

FileTransferBridge использует TCP-порты 30522 и 30523. Порты прослушивают только интерфейс localhost (127.0.0.1) и не принимают входящие подключения из внешних сетей.

HTTPS

Безопасный протокол передачи данных между браузером и веб-сервером с использованием шифрования. HTTPS используется для доступа к закрытой информации, такой как корпоративные или финансовые данные.

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.

iOS MDM-профиль

Набор параметров подключения мобильных устройств iOS к Серверу администрирования. iOS MDM-профиль устанавливается пользователем на мобильное устройство, после чего это мобильное устройство подключается к Серверу администрирования.

iOS MDM-устройство

Мобильное устройство, которое подключается к Серверу iOS MDM по протоколу iOS MDM. По протоколу iOS MDM могут подключаться и управляться устройства с операционной системой iOS.

JavaScript

Язык программирования, расширяющий возможности веб-страниц. Веб-страницы, созданные с использованием JavaScript, способны выполнять дополнительные действия (например, изменять вид элементов интерфейса или открывать дополнительные окна) без обновления веб-страницы данными с веб-сервера. Чтобы просматривать веб-страницы, созданные с использованием JavaScript, в параметрах браузера надо включить поддержку JavaScript.

Kaspersky Security Center System Health Validator (SHV)

Компонент приложения Kaspersky Security Center, предназначенный для проверки работоспособности операционной системы при совместной работе приложения Kaspersky Security Center с Microsoft NAP.

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.

KES-устройство

Мобильное устройство, которое подключается к Серверу администрирования и управляется с помощью мобильного приложения Kaspersky Endpoint Security для Android.

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.

MITM-атака

Man in The Middle (человек посередине). Атака на IT-инфраструктуру организации, при которой злоумышленник перехватывает канал связи между двумя точками доступа, ретранслирует и при необходимости изменяет связь между этими точками доступа.

Network Location Awareness (NLA)

Служба Windows, которая помогает операционной системе идентифицировать текущую сеть. NLA обнаруживает изменения в сети и настраивает конфигурацию безопасности устройства.

Provisioning-профиль

Набор параметров для работы приложений на мобильных устройствах iOS. Provisioning-профиль содержит информацию о лицензии и привязан к конкретному приложению.

SSL

Протокол шифрования данных в локальных сетях и в интернете. SSL используется в веб-приложениях для создания защищенных соединений между клиентом и сервером.

Windows Server Update Services (WSUS)

Приложение, которое используется для распространения обновлений приложений Microsoft на компьютерах пользователей в сети организации.

Агент администрирования

Компонент приложений Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования и приложениями "Лаборатории Касперского", установленными на конкретном сетевом узле (рабочей станции или сервере). Этот компонент является единым для всех приложений компании для Windows. Для приложений "Лаборатории Касперского" для Novell®, Unix™ и Mac существуют отдельные версии Агента администрирования.

Агент аутентификации

Интерфейс, позволяющий после шифрования загрузочного жесткого диска пройти процедуру аутентификации для доступа к зашифрованным жестким дискам и для загрузки операционной системы.

Агент обновлений

Устройство с установленным Агентом администрирования, которое используется для распространения обновлений, удаленной установки приложений, получения информации об устройствах в составе группы администрирования и/или широковещательного домена. Агенты обновлений предназначены для уменьшения нагрузки на Сервер администрирования при распространении обновлений и для оптимизации трафика в сети. Агенты обновлений могут быть назначены автоматически Сервером администрирования или вручную администратором.

Административные права

Уровень прав и полномочий пользователя для администрирования объектов Exchange внутри организации Exchange.

Администратор Kaspersky Security Center

Лицо, управляющее работой приложения через систему удаленного централизованного администрирования Kaspersky Security Center.

Администратор клиента

Сотрудник организации-клиента, который отвечает за обеспечение антивирусной безопасности организации-клиента.

Администратор поставщика услуг

Сотрудник организации-поставщика услуг антивирусной защиты. Выполняет работы по инсталляции, эксплуатации систем антивирусной защиты, созданных на основе решений "Лаборатории Касперского", а также осуществляет техническую поддержку клиентов.

Активный ключ

Ключ, используемый в текущий момент для работы приложения.

Антивирусная безопасность сети

Комплекс технических и организационных мер, снижающих вероятность проникновения на устройства сети организации вирусов и спама, предотвращающих сетевые атаки, фишинг и другие угрозы. Антивирусная безопасность сети повышается при использовании приложений защиты и сервисов, а также при наличии и соблюдении политики информационной безопасности в организации.

Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать в проверяемых объектах вредоносный код. Антивирусные базы формируются специалистами "Лаборатории Касперского" и обновляются каждый час.

Веб-сервер Kaspersky Security Center

Компонент Kaspersky Security Center, который устанавливается в составе Сервера администрирования. Веб-сервер предназначен для передачи по сети автономных пакетов установки, iOS MDM-профилей, а также файлов из папки общего доступа.

Виртуальный Сервер администрирования

Компонент приложения Kaspersky Security Center, предназначенный для управления системой защиты сети организации-клиента.

Виртуальный Сервер администрирования является частным случаем подчиненного Сервера администрирования и, по сравнению с физическим Сервером администрирования, имеет следующие основные ограничения:

- Виртуальный Сервер администрирования может функционировать только в составе главного Сервера администрирования.
- Виртуальный Сервер администрирования при работе использует основную базу данных главного Сервера администрирования. Задачи резервного копирования и восстановления данных, а также задачи проверки и загрузки обновлений, не поддерживаются на виртуальном Сервере администрирования.
- Для виртуального Сервера не поддерживается создание подчиненных Серверов администрирования (в том числе и виртуальных).

Вирусная атака

Ряд целенаправленных попыток заразить устройство вирусом.

Владелец устройства

Владелец устройства – это пользователь устройства, с которым администратор может контактировать в случае необходимости выполнить какие-либо работы с устройством.

Внутренние пользователи

Учетные записи внутренних пользователей используются для работы с виртуальными Серверами администрирования. Под именем учетной записи внутреннего пользователя администратор виртуального Сервера может запускать Kaspersky Security Center Web Console для просмотра сведений о состоянии антивирусной безопасности сети. В рамках функциональности приложения Kaspersky Security Center внутренние пользователи обладают правами реальных пользователей.

Учетные записи внутренних пользователей создаются и используются только внутри Kaspersky Security Center. Сведения о внутренних пользователях не передаются операционной системе. Аутентификацию внутренних пользователей осуществляет Kaspersky Security Center.

Восстановление

Перемещение оригинального объекта из карантина или резервного хранилища в папку его исходного расположения, где объект хранился до его помещения на карантин, лечения или удаления, либо другую папку, указанную пользователем.

Восстановление данных Сервера администрирования

Восстановление данных Сервера администрирования при помощи утилиты резервного копирования на основании информации, сохраненной в резервном хранилище. Утилита позволяет восстанавливать:

- информационную базу Сервера администрирования (политики, задачи, параметры приложения, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов приложений для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором приложений "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждого из установленных в группе приложений могут быть созданы групповые политики и сформированы групповые задачи.

Группа лицензионных программ

Группа программ, созданная на основании заданных администратором критериев (например, по производителю), для которых ведется учет установок на клиентских устройствах.

Групповая задача

Задача, определенная для группы администрирования и выполняемая на всех клиентских устройствах, входящих в состав этой группы администрирования.

Демилитаризованная зона (DMZ)

Демилитаризованная зона – это сегмент локальной сети, в которой находятся серверы, отвечающие на запросы из глобальной сети. В целях обеспечения безопасности локальной сети организации доступ в локальную сеть из демилитаризованной зоны ограничен и защищен сетевым экраном.

Домашний Сервер администрирования

Домашний Сервер администрирования – это Сервер администрирования, который был задан при установке Агента администрирования. Домашний Сервер администрирования может использоваться в параметрах профилей подключения Агента администрирования.

Дополнительный ключ

Ключ, подтверждающий право на использование приложения, но не используемый в текущий момент.

Доступное обновление

Пакет обновлений модулей приложения "Лаборатории Касперского", в состав которого включены набор срочных обновлений, собранных за некоторый период, и изменения в архитектуре приложения.

Задача

Функции, выполняемые приложением "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

Задача для набора устройств

Задача, определенная для набора клиентских устройств из произвольных групп администрирования и выполняемая на них.

Инсталляционный пакет

Набор файлов, формируемый для удаленной установки приложения "Лаборатории Касперского" при помощи системы удаленного управления Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки приложения и обеспечения его работоспособности сразу после установки. Значения параметров соответствуют значениям параметров приложения по умолчанию. Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива приложения.

Инстанс Amazon EC2

Виртуальная машина, созданная на основе образа AMI с использованием Amazon Web Services.

Клиент Сервера администрирования (Клиентское устройство)

Устройство, сервер или рабочая станция, на котором установлены Агент администрирования и управляемые приложения "Лаборатории Касперского".

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/.

Консоль администрирования

Компонент приложения Kaspersky Security Center, предоставляющий пользовательский интерфейс к административным службам Сервера администрирования и Агента администрирования.

Конфигурационный профиль

Политика, содержащая набор параметров и ограничений для мобильного устройства iOS MDM.

Локальная задача

Задача, определенная и выполняющаяся на отдельном клиентском устройстве.

Локальная установка

Установка приложения защиты на устройство сети организации, которая предусматривает ручной запуск установки из дистрибутива приложения защиты или ручной запуск опубликованного инсталляционного пакета, предварительно загруженного на устройство.

Магазин приложений

Компонент приложения Kaspersky Security Center. Магазин приложений используется для установки приложений на Android-устройства пользователей. В магазине приложений можно публиковать apk-файлы приложений и ссылки на приложения в Google Play.

Настройки задачи

Настройки работы приложения, специфичные для каждого типа задач.

Непосредственное управление приложением

Управление приложением через локальный интерфейс.

Несовместимое приложение

Антивирусное приложение стороннего производителя или приложение "Лаборатории Касперского", не поддерживающее управление через Kaspersky Security Center.

Облачное окружение

Виртуальные машины на базе облачной платформы, объединенные в сети.

Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений "Лаборатории Касперского".

Обновление приложения Kaspersky Security Center

Процедура установки новой версии Kaspersky Security Center на устройство, на котором установлена более ранняя версия этого приложения.

Образ AMI

Шаблон с необходимой для запуска виртуальной машины конфигурацией программного обеспечения. На основе одного образа AMI можно создать несколько инстансов.

Общий сертификат

Сертификат, предназначенный для идентификации мобильного устройства пользователя.

Оператор Kaspersky Security Center

Пользователь, который ведет наблюдение за состоянием и работой системы защиты, управляемой при помощи Kaspersky Security Center.

Параметры приложения

Параметры работы приложения, общие для всех типов его задач и отвечающие за работу приложения в целом, например: параметры производительности приложения, параметры ведения отчетов, параметры резервного хранилища.

Плагин управления приложением

Специализированный компонент, предоставляющий интерфейс для управления работой приложения через Консоль администрирования. Для каждого приложения существует свой плагин управления. Он входит в состав всех приложений "Лаборатории Касперского", управление которыми может осуществляться при помощи Kaspersky Security Center.

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.

Поставщик услуг антивирусной защиты

Организация, предоставляющая услуги антивирусной защиты сетей организации-клиента на основе решений "Лаборатории Касперского".

Рабочее место администратора

Устройство, на котором установлена Консоль администрирования – компонент, предоставляющий интерфейс управления Kaspersky Security Center.

С рабочего места администратор управляет серверной частью Kaspersky Security Center: выстраивает систему централизованной защиты сети организации, сформированную на базе приложений "Лаборатории Касперского", и контролирует ее.

Резервное копирование данных Сервера администрирования

Копирование данных Сервера администрирования для резервного хранения и последующего восстановления, осуществляемое при помощи утилиты резервного копирования. Утилита позволяет сохранять:

- информационную базу Сервера администрирования (политики, задачи, параметры приложения, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов приложений для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

Руководство по усилению защиты

Рекомендации и особенности настройки Kaspersky Security Center и его компонентов для снижения рисков его компрометации.

Ручная установка

Установка приложения защиты на устройство сети организации из дистрибутива приложения защиты. Ручная установка требует непосредственного участия администратора или другого IT-специалиста. Обычно ручная установка применяется, если удаленная установка завершилась с ошибкой.

Сервер iOS MDM

Компонент Kaspersky Security Center, который устанавливается на клиентское устройство и позволяет подключать мобильные устройства iOS к Серверу администрирования и управлять ими с помощью сервиса Apple Push Notifications (APNs).

Сервер администрирования

Компонент приложения Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации приложениях "Лаборатории Касперского" и управления ими.

Сервер мобильных устройств

Компонент Kaspersky Security Center, который предоставляет доступ к мобильным устройствам и позволяет управлять ими через Консоль администрирования.

Серверы обновлений "Лаборатории Касперского"

HTTP-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложения.

Сертификат Сервера администрирования

Сертификат, на основании которого осуществляется аутентификация Сервера администрирования при подключении к нему Консоли администрирования и обмене информацией с клиентскими устройствами. Сертификат Сервера администрирования создается при установке Сервера администрирования и хранится на Сервере администрирования в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

Состояние защиты

Текущее состояние защиты, характеризующее степень защищенности устройства.

Состояние защиты сети

Текущее состояние защиты, характеризующее степень защищенности устройств сети организации. Состояние защиты сети включает такие факторы, как наличие на устройствах сети установленных приложений защиты, использование ключей, количество и виды обнаруженных угроз.

Срок действия лицензии

Период времени, в течение которого вы можете пользоваться функциями приложения и дополнительными услугами. Объем доступных функций и дополнительных услуг зависит от типа лицензии.

Удаленная установка

Установка приложений "Лаборатории Касперского" при помощи инструментов, предоставляемых приложением Kaspersky Security Center.

Управляемые устройства

Устройства сети организации, включенные в одну из групп администрирования.

Уровень важности патча

Характеристика патча. Для патчей сторонних производителей или Microsoft существует пять уровней важности:

- Предельный.
- Высокий.
- Средний.
- Низкий.
- Неизвестно.

Уровень важности патча стороннего производителя или Microsoft определяется наиболее неблагоприятным уровнем критичности уязвимости, которую закрывает патч.

Уровень важности события

Характеристика события, зафиксированного в работе приложения "Лаборатории Касперского". Существуют четыре уровня важности:

- Критическое событие.
- Отказ функционирования.
- Предупреждение.
- Информационное сообщение.

События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

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.

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 резервных копий

Специальная папка для сохранения копий данных Сервера администрирования, создаваемых при помощи утилиты резервного копирования.

Хранилище событий

Часть базы данных Сервера администрирования, предназначенная для хранения информации о событиях, которые возникают в Kaspersky Security Center.

Централизованное управление приложением

Удаленное управление приложением при помощи сервисов администрирования, предоставляемых Kaspersky Security Center.

Широковещательный домен

Логический участок компьютерной сети, в котором все узлы могут передавать данные друг другу с помощью широковещательного канала на уровне сетевой модели OSI (Open Systems Interconnection Basic Reference Model).

Шлюз соединения

Шлюз соединения – это Агент администрирования, работающий в особом режиме. Шлюз соединения принимает соединения от других Агентов администрирования и туннелирует их к Серверу администрирования через собственное соединение с Сервером. В отличие от обычного Агента администрирования, шлюз соединения ожидает соединений от Сервера администрирования, а не устанавливает соединения с Сервером администрирования.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки приложения.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe, Acrobat, Flash, Shockwave и PostScript являются либо зарегистрированными товарными знаками, либо товарными знаками компании Adobe в США и/или других странах.

AMD, AMD64 – товарные знаки или зарегистрированные товарные знаки Advanced Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace являются товарными знаками Amazon.com, Inc. или аффилированных лиц компании.

Apache является либо зарегистрированным товарным знаком, либо товарным знаком Apache Software Foundation в Соединенных Штатах и/или других странах.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime и Touch ID – товарные знаки Apple Inc.

Arm – зарегистрированный товарный знак Arm Limited (или дочерних компаний) в США и/или других странах.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Ubuntu, LTS являются зарегистрированными товарными знаками Canonical Ltd.Cisco Systems, Cisco, Cisco Jabber, IOS являются зарегистрированными товарными знаками или товарными знаками Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

Citrix, XenServer являются зарегистрированными товарными знаками или товарными знаками Cloud Software Group, Inc. и/или дочерних компаний в США и/или других странах.

Corel – товарный знак или зарегистрированный в Канаде, США и/или других странах товарный знак Corel Corporation и/или ее дочерних компаний.

Cloudflare, логотип Cloudflare и Cloudflare Workers являются товарными знаками и/или зарегистрированными товарными знаками компании Cloudflare, Inc. в США и других юрисдикциях.

Dropbox – товарный знак Dropbox, Inc.

Radmin – зарегистрированный товарный знак Famatech.

Firebird – зарегистрированный товарный знак Firebird Foundation.

Foxit – зарегистрированный товарный знак Foxit Corporation.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Hangouts, Google Public DNS и YouTube – товарные знаки Google LLC.

EulerOS, FusionCompute, FusionSphere являются товарными знаками Huawei Technologies Co., Ltd.

Intel, Core, Xeon являются товарными знаками Intel Corporation или ее дочерних компаний.

IBM, QRadar – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Node.js – товарный знак Joyent, Inc.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Logitech является зарегистрированным товарным знаком или товарным знаком компании Logitech в США и (или) других странах.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, Office 365, PowerShell, PowerPoint, SharePoint, SQL Server, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Mobile, Windows Server, Windows Phone, Windows Vista и Windows Azure 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.

OpenSSL является товарным знаком правообладателя OpenSSL Software Foundation.

Oracle, Java, JavaScript и TouchDown – зарегистрированные товарные знаки компании Oracle и/или аффилированных компаний.

Parallels, логотип Parallels и Coherence являются товарными знаками или зарегистрированными товарными знаками Parallels International GmbH.

Chef – товарный знак или зарегистрированный в США и/или других странах товарный знак Progress Software Corporation и/или одной из дочерних или аффилированных компаний.

Puppet – товарный знак или зарегистрированный товарный знак Puppet, Inc.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

Red Hat, Fedora и Red Hat Enterprise Linux – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

Ansible является зарегистрированным товарным знаком Red Hat, Inc. в США и других странах.

CentOS – товарный знак или зарегистрированный в США и других странах товарный знак Red Hat, Inc. или дочерних компаний.

BlackBerry принадлежит Research In Motion Limited, зарегистрирован в США и может быть подан на регистрацию или зарегистрирован в других странах.

Rocky Linux является товарным знаком The Rocky Enterprise Software Foundation.

SAMSUNG – товарный знак компании SAMSUNG в США или других странах.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

Splunk, SPL – товарные знаки и зарегистрированные в США и других странах товарные знаки Splunk, Inc.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

Владельцем товарного знака Symbian является Symbian Foundation Ltd.

OpenAPI – товарный знак компании The Linux Foundation.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

Zabbix – зарегистрированный товарный знак Zabbix SIA.

Известные проблемы и ограничения

Kaspersky Security Center Web Console имеет ряд ограничений, не критичных для работы приложения:

- 10671377: При использовании PostgreSQL и Postgres Pro версий 18.1-18.5 запущенные задачи могут завершаться с ошибкой "'[53000]' ERROR: no empty local buffer available". Рекомендуется обновить PostgreSQL до версии 18.6, либо выполнить следующие действия:

  1. Остановите службу Сервера администрирования.
  2. Остановите службу СУБД.
  3. В конец файла postgresql.conf добавьте следующую строку: `effective_io_concurrency=0`.
  4. Запустите службу СУБД.
  5. Убедитесь, что значение параметра `effective_io_concurrency` равно `0` с помощью следующего запроса:
     `SELECT setting FROM pg_settings WHERE name = 'effective_io_concurrency';`
  6. Запустите службу Сервера администрирования.

- 10746086: При первом запуске Агент администрирования всегда пытается запустить службу Центр обновления Windows. В случае, если служба отключена, в Журнале Kaspersky Event Log появится событие о недоступности службы Центр обновления Windows. Если служба отключена специально, и функционал поиска обновлений Windows не требуется, в политике Агента администрирования на вкладке **Хранилища** рекомендуется отключить параметр **Информация об обновлениях Центра обновления Windows**.

- 9838414: Установка Агента администрирования для Microsoft Windows на Arm с помощью автономного инсталляционного пакета может остаться на шаге **Проверка подключения к Серверу администрирования**, хотя устройство успешно подключено к Серверу администрирования и установка завершена. Если установка осталась на этом шаге, вы можете закрыть окно мастера установки. Агент администрирования для Microsoft Windows на Arm уже установлен.

- 9978211: Параметр **Использовать в качестве шлюза соединения в демилитаризованной зоне** не поддерживается для Microsoft Windows на Arm.

- Изменения, внесенные в расписание задачи, не распространяются на управляемые устройства, если в расписании используется параметр **По дням недели**. Если нужно изменить расписание, удалите существующую задачу и создайте другую с обновленными параметрами.

- Информация о компонентах управляемых приложений недоступна, если Агент администрирования установлен на устройстве с операционной системой Microsoft Windows XP.

- Подраздел **Алерты** раздела **Мониторинг и отчеты** отображается в главном меню, только если вы добавили лицензионный ключ для EDR Optimum в хранилище Сервера администрирования, введя код активации.

- Для обеспечения криптографической стойкости сертификат Сервера администрирования должен быть подписан с использованием SHA-2 и иметь минимальную длину ключа 2048. Если вам нужно перевыпустить сертификат, см. Базу знаний Kaspersky Security Center.

- Если вы создаете задачу с параметрами расписания **Каждые N дней** и **По дням недели** в Kaspersky Security Center 15.1 Web Console, а затем открываете задачу в более ранних версиях Kaspersky Security Center Web Console или Консоли администрирования Kaspersky Security Center (например, когда задача также применяется на подчиненных Серверах администрирования, которые могут быть как с операционной системой Linux, так и с Windows), параметры расписания могут отображаться некорректно или может произойти ошибка.

- Когда вы настраиваете экспорт в SIEM-системы в Kaspersky Security Center Web Console и выбираете UDP-протокол, после нажатия на кнопку **Проверить соединение** возвращается ошибка, так как UDP не устанавливает соединение и доставка данных не может быть гарантирована.

- При запуске задачи по удалению Агента администрирования на устройстве на базе архитектуры Arm и работающего на Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7), Агент администрирования успешно удаляется, но статус задачи для текущего прогресса в списке задач заморожен.

- Окно свойств Kaspersky Device Management для iOS еще содержит раздел **Параметры EAS-устройств**, хотя Exchange ActiveSync больше не поддерживается.

- Не удается выполнить подключение к KSN через HTTPS, если Kaspersky Security Center установлен на устройстве с кириллическими символами в названии устройства и прокси-сервер KSN включен на Сервере администрирования.

- Когда вы пытаетесь изменить свойства учетной записи пользователя с включенным параметром **Запрашивать аутентификацию для проверки разрешения на изменение учетных записей пользователей**, а затем нажимаете на кнопку **Отмена** в окне **Защита учетной записи**, происходит неожиданная ошибка.

- При изменении времени или часовой зоны на устройстве необходимо перезапустить службу Kaspersky Security Center Web Console.

- Если на устройстве используется прокси-сервер и заданы переменные окружения прокси-сервера, приложение установки Kaspersky Security Center Web Console может зависнуть.

- 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 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.

- Клиентские устройства могут быть не найдены после запуска опроса сети Windows.

- Если в мастере **Add secondary Administration Server** указать учетную запись с включенной двухэтапной проверкой для аутентификации, на будущем подчиненном Сервере, мастер завершает работу с ошибкой. Чтобы решить эту проблему, укажите учетную запись, для которой отключена двухфакторная аутентификация, или создайте иерархию из будущего подчиненного Сервера.

- При входе в Kaspersky Security Center Web Console, если вы используете доменную аутентификацию и указываете виртуальный Сервер администрирования для подключения, затем выходите из приложения и пытаетесь войти на главный Сервер администрирования, Kaspersky Security Center Web Console все равно подключается к виртуальному Серверу администрирования. Чтобы подключиться к главному Серверу администрирования, повторно откройте браузер.

- Быстрый/полный опрос сети Windows возвращает пустой результат.
- Если вы устанавливаете Kaspersky Security Center Web Console с Identity and Access Manager, а затем меняете Сервер администрирования Kaspersky Security Center Web Console, компонент Identity and Access Manager не получает информацию о новом Сервере администрирования.
- Управляемое устройство, имеющее более одного сетевого адаптера, отправляет Серверу администрирования информацию о MAC-адресе сетевого адаптера, отличного от того, который используется для подключения к Серверу администрирования.
- Тестовое подключение к SIEM-системе завершается ошибкой при выборе формата данных CEF.
- NTLM-аутентификация не работает для учетных записей пользователей группы "Защищенные пользователи".